VICON

Installation Guide

XX268-20-01

CE102B Network Outdoor Bullet Camera

Vicon Industries Inc.

Tel: 631-952-2288 Fax: 631-951-2288 Toll Free: 800-645-9116

24-Hour Technical Support: 800-34-VICON (800-348-4266) UK: 44/(0) 1489-566300

Vicon Industries Inc. does not warrant that the functions contained in this equipment will meet your requirements or that the operation will be entirely error free or perform precisely as described in the documentation. This system has not been designed to be used in life-critical situations and must not be used for this purpose.

www.vicon-security.com

Document Number: 8009-8268-20-01

Issued: 714

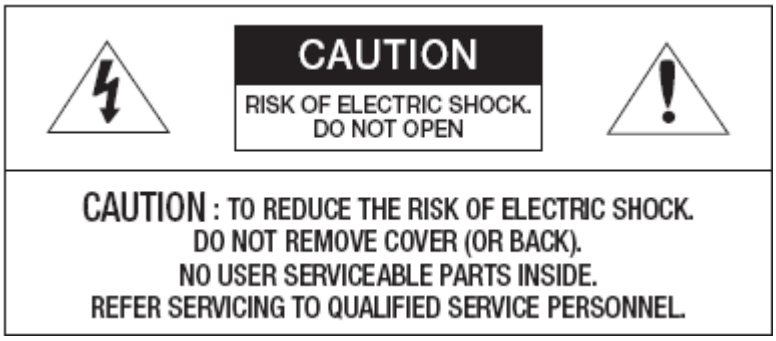
Product specifications subject to change without notice.

Copyright © 2014 Vicon Industries Inc. All rights reserved.

WARNING

TO REDUCE THE RISK OF FIRE OR ELECTRIC SHOCK, DO NOT INSERT ANY METALLIC OBJECT THROUGH THE VENTILATION GRILLS OR OTHER OPENINGS ON THE EQUIPMENT.

CAUTION


CAUTION
RISK OF ELECTRIC SHOCK.
DO NOT OPEN
CAUTION : TO REDUCE THE RISK OF ELECTRIC SHOCK.
DO NOT REMOVE COVER (OR BACK).
NO USER SERVICEABLE PARTS INSIDE.
REFER SERVICING TO QUALIFIED SERVICE PERSONNEL.

EXPLANATION OF GRAPHICAL SYMBOLS

The lightning flash with arrowhead symbol, within an equilateral triangle, is intended to alert the user to the presence of uninsulated "dangerous voltage" within the product's enclosure that may be of sufficient magnitude to constitute a risk of electric shock.

The exclamation point within an equilateral triangle is intended to alert the user to the presence of important operating and maintenance (servicing) instructions in the literature accompanying the appliance.

PRECAUTIONS

Safety ---------- Installation ----------

Should any liquid or solid object fall into the cabinet, unplug the unit and have it checked by the qualified personnel before operating it any further.

Unplug the unit from the wall outlet if it is not going to be used for several days or more. To disconnect the cord, pull it out by the plug. Never pull the cord itself.

Allow adequate air circulation to prevent internal heat build-up. Do not place the unit on surfaces (rugs, blankets, etc.) or near materials (curtains, draperies) that may block the ventilation holes.

Height and vertical linearity controls located at the rear panel are for special adjustments by qualified personnel only.

Before installation, carefully read the manual to ensure correct operation and setup, heeding all warnings and instructions.

Do not install the device near any heat sources such as radiators, heat registers, stoves, or other equipment (including amplifiers) that produce heat.

Only use attachments/accessories specified by the manufacturer.

Do not install the device in a place where it is exposed to gas or oil.

Cleaning ----------

Clean the unit with a slightly damp soft cloth.
Use a mild household detergent. Never use strong solvents such as thinner or benzene as they might damage the finish of the unit.

Retain the original carton and packing materials for safe transport of this unit in the future.

FCC COMPLIANCE STATEMENT

INFORMATION TO THE USER: THIS EQUIPMENT HAS BEEN TESTED AND FOUND TO COMPLY WITH THE LIMITS FOR A CLASS A DIGITAL DEVICE, PURSUANT TO PART 15 OF THE FCC RULES. THESE LIMITS ARE DESIGNED TO PROVIDE REASONABLE PROTECTION AGAINST HARMFUL INTERFERENCE WHEN THE EQUIPMENT IS OPERATED IN A COMMERCIAL ENVIRONMENT. THIS EQUIPMENT GENERATES, USES, AND CAN RADIATE RADIO FREQUENCY ENERGY AND IF NOT INSTALLED AND USED IN ACCORDANCE WITH THE INSTRUCTION MANUAL, MAY CAUSE HARMFUL INTERFERENCE TO RADIO COMMUNICATIONS.

CAUTION: CHANGES OR MODIFICATIONS NOT EXPRESSLY APPROVED BY THE PARTY RESPONSIBLE FOR COMPLIANCE COULD VOID THE USER'S AUTHORITY TO OPERATE THE EQUIPMENT.

THIS CLASS A DIGITAL APPARATUS COMPLIES WITH CANADIAN ICES-003.

CET APPAREIL NUMÉRIQUE DE LA CLASSE A EST CONFORME À LA NORME NMB-003 DU CANADA.

CE COMPLIANCE STATEMENT

WARNING: This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

IMPORTANT SAFETY INSTRUCTIONS

1. Read these instructions.
2. Keep these instructions.
3. Heed all warnings.
4. Follow all instructions.
5. Do not use this apparatus near water.
6. Clean only with dry cloth.
7. Do not block any ventilation openings. Install in accordance with the manufacturer's instructions.
8. Do not install near any heat sources such as radiators, heat registers, stoves, or other apparatus (including amplifiers) that produce heat.
9. Do not defeat the safety purpose of the polarized or grounding-type plug. A polarized plug has two blades with one wider than the other. A grounding type plug has two blades and a third grounding prong. The wide blade or the third prong is provided for your safety. If the provided plug does not fit into your outlet, consult an electrician for replacement of the obsolete outlet.
10. Protect the power cord from being walked on or pinched particularly at plugs, convenience receptacles, and the point where they exit from the apparatus.
11. Only use attachments/accessories specified by the manufacturer.
12. Use only with the cart, stand, tripod, bracket, or table specified by the manufacturer, or sold with the apparatus. When a cart is used, use caution when moving the cart/apparatus combination to avoid injury from tip-over.
13. Unplug this apparatus during lightning storms or when unused for long periods of time.

14. Refer all servicing to qualified service personnel. Servicing is required when the apparatus has been damaged in any way, such as power-supply cord or plug is damaged, liquid has been spilled or objects have fallen into the apparatus, the apparatus has been exposed to rain or moisture, does not operate normally, or has been dropped.
15. ***CAUTION – THESE SERVICING INSTRUCTIONS ARE FOR USE BY QUALIFIED SERVICE PERSONNEL ONLY. TO REDUCE THE RISK OF ELECTRIC SHOCK DO NOT PERFORM ANY SERVICING OTHER THAN THAT CONTAINED IN THE OPERATING INSTRUCTIONS UNLESS YOU ARE QUALIFIED TO DO SO.***
16. ***Use satisfy clause 2.5 of IEC60950-1/UL60950-1 or Certified/Listed Class 2 power source only.***
17. ITE is to be connected only to PoE networks without routing to the outside plant.

Contents

1. Description ----------6
1.1 Components - ---------- 6
1.2 Key Features - ---------- 7

2. Installation ---------- 8
2.1 Camera Installation ---- ---------- 8
2.2 Connection ---- ---------- 9
2.3 Network Connection and IP Assignment ---------- 10

3. Operation ---------- 11
3.1 Access from a browser ---------- 11
3.2 Access from the internet ---------- 12
3.3 Setting the admin password over a secure connection ---------- 12
3.4 Live View Page ---------- 12
3.5 Network Camera Setup ---------- 14
3.5.1 Basic Configuration ---------- 14
1) Users ---------- 15
2) Network ---------- 16
3) Video & Image ---------- 17
4) Date & Time ---------- 19
3.5.2 Live View ---------- 20
3.5.3 Video & Image ---------- 21
3.5.4 Event ---------- 27
1) Event-In ---------- 27
2) Event-Out ---------- 32
3) Event Map ---------- 37
3.5.5 System ---------- 39
1) Information ---------- 39
2) Security ---------- 40
3) Date & Time ---------- 45
4) Network ---------- 46
5) Language ---------- 55
6) Maintenance ---------- 56
7) Support ---------- 57
3.6 Playback ----------60
3.7 Help ---------- 62
3.8 Resetting to the factory default settings ---------- 63

4. Appendix ---------- 64
4.1 Troubleshooting ---------- 64
4.2 Preventive Maintenance ---------- 65
4.3 Product Specification ---------- 66

1. Description

The information in this manual provides quick installation and setup procedures for the CE102B-NIR Bullet Camera. These units should only be installed by a qualified technician using approved materials in conformance with federal, state, and local codes. Read these instructions thoroughly before beginning an installation. Always refer to Vicon's website to assure you have the most up-to-date manual, www.vicon-security.com.

The CE102B-NIR HD IP Bullet Camera is designed for demanding security installations. This cost-effective fixed network camera includes an integral 3.7 mm megapixel fixed lens; the 1080p resolution delivers crisp clear images. The CE102B-NIR cameras are fully compatible with all ViconNet® systems; its ONVIF certification provides an open-platform for integration into other video management systems.

The network camera provides triple-streaming video and supports H.264 compression technology. MPEG-4 and Motion JPEG (M-JPEG) compressions are also provided. Installation is made easy and cost-effective with Power-over-Ethernet (PoE); the camera also accepts 12 VDC. The CE102B-NIR automatically adapts to changing outdoor lighting; the true day/night camera includes a removable IR cut filter. Built-in IR LEDs provide illumination up to 65 ft (20 m). The camera is IP67 rated with a vandal-proof casing that withstands rain, dust and vandalism.

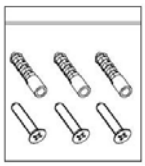
1.1 Components

The system comes with the following components:

Camera Unit

Installation CD

Installation Guide



Accessory Kit

Notes:

1. Check your package to make sure that you received the complete system, including all components shown above.
2. Adapter for 12 VDC is not supplied.

1.2 Key Features

- **Brilliant video quality**
  The network camera offers the highly efficient H.264 video compression, which drastically reduces bandwidth and storage requirements without compromising image quality. Motion JPEG is also supported for increased flexibility.

- **Triple streams**
  The network camera can deliver triple video streams simultaneously at full frame rate in all resolutions up to 1920 x 1080 using Motion JPEG and H.264 (or MPEG-4). This means that several video streams can be configured with different compression formats, resolutions and frame rates for different needs.

- **Image setting adjustment**
  The network camera also enables users to adjust image settings such as contrast, brightness and saturation to improve images before encoding takes place.

- **Micro-SD Recording support**
  The network camera also supports a micro-SD memory slot for local recording with removable storage.

- **Improved Security**
  The network camera logs all user access, and lists currently connected users. Also, its full frame rate video can be provided over HTTPS.

- **Megapixel Resolution**
  Max 30fps@1920x1080.

- **Power over Ethernet**
  Support for Power over Ethernet (IEEE802.3af) enables the unit, as well as the camera module that is connected to it, to receive power through the same cable as for data transmission. This makes for easy installation since no power outlet is needed.

- **ONVIF**
  This is a global interface standard that makes it easier for end users, integrators, consultants, and manufacturers to take advantage of the possibilities offered by network video technology. ONVIF enables interoperability between different vendor products, increased flexibility, reduced cost, and future-proof systems.

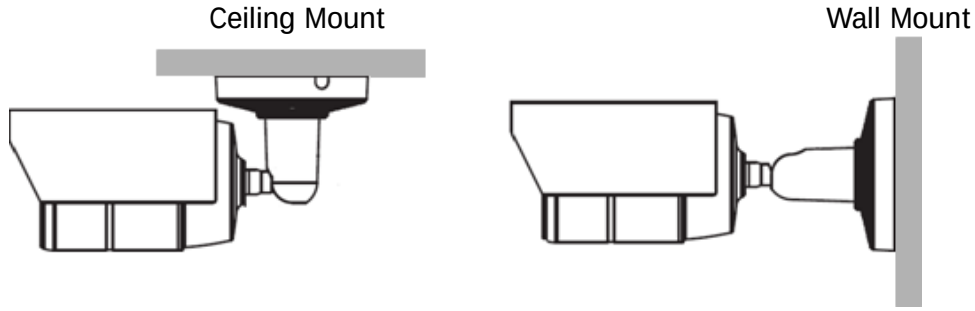
2. Installation

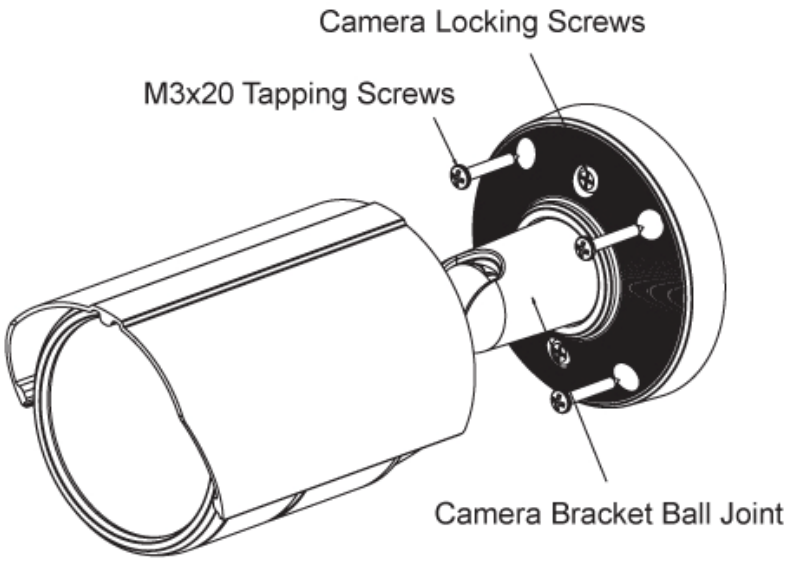
2.1 Camera Installation

Carefully remove the contents from the box and verity that nothing was damaged in shipment.

- **Base Installation**
  1. Create a hole in the mounting surface for the cables. Route the necessary cables to the mounting location.
  2. Secure the camera mounting base to the wall or ceiling using the screws supplied in the accessory kit.

Note: Make sure the mounting surface is strong enough to support the weight of the unit.





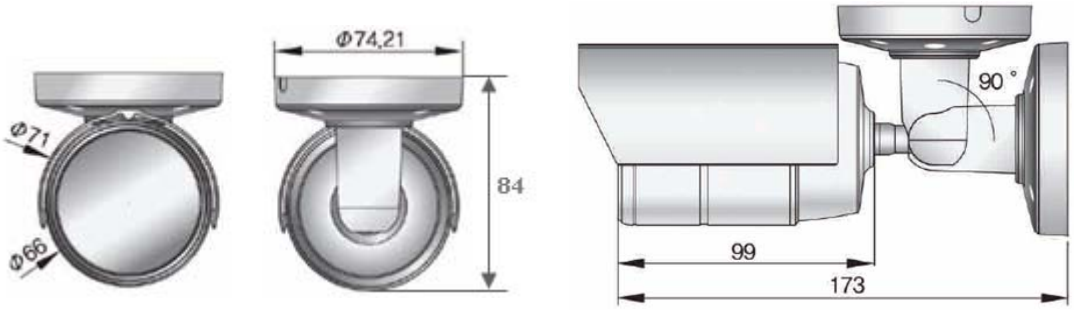
Caution

Adjust the position of the camera before securing it in place;
adjusting the position after installation could damage the cable.

Loosen the Camera Locking Screws (2X) and position the bullet camera
When adjustment is complete, tighten the screws to lock into place.

- **Camera Dimension**

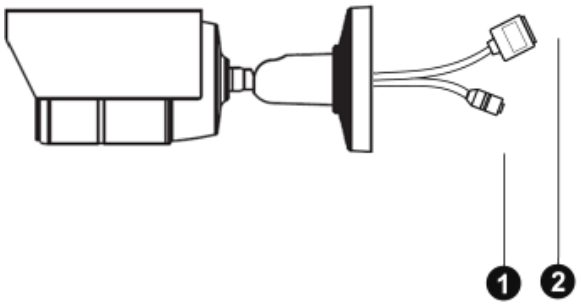
See the diagrams below for the exact dimension



Dimensions Unit: mm

2.2 Connections

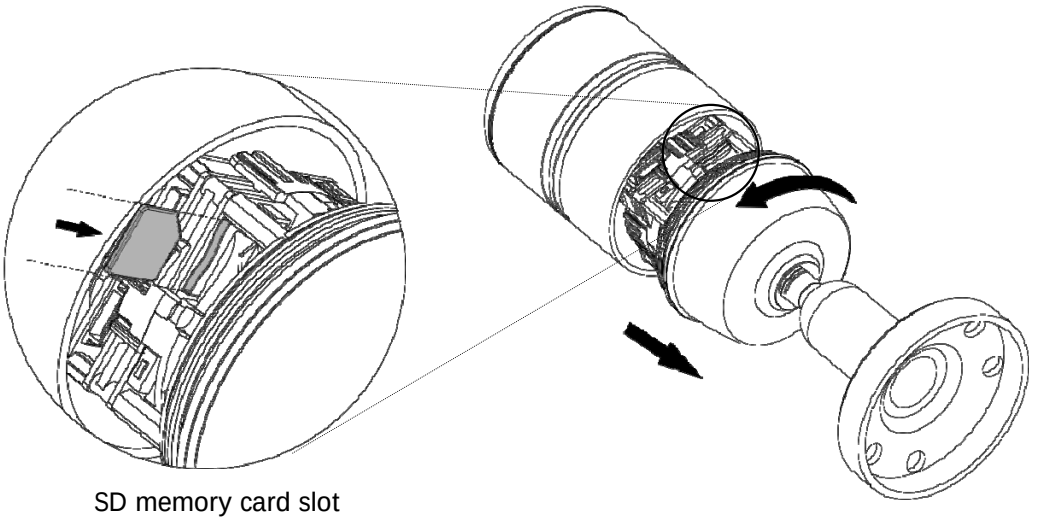
- **Connection Cable**



NO	Name	Description
1	Power Cable	Cable for Power source (12 VDC)
2	Ethernet Cable	Cable for Ethernet (PoE)

- **Connecting to the RJ-45**
  Connect a standard RJ-45 cable to the network port of the network camera. Generally a cross-over cable is used for directly connection to PC, while a direct cable is used for connection to a hub or switch.

- **Micro SD memory slot**
  Remove the front cap of the camera to insert the SD memory card (customer-supplied).



SD memory card slot

Remove the front cap

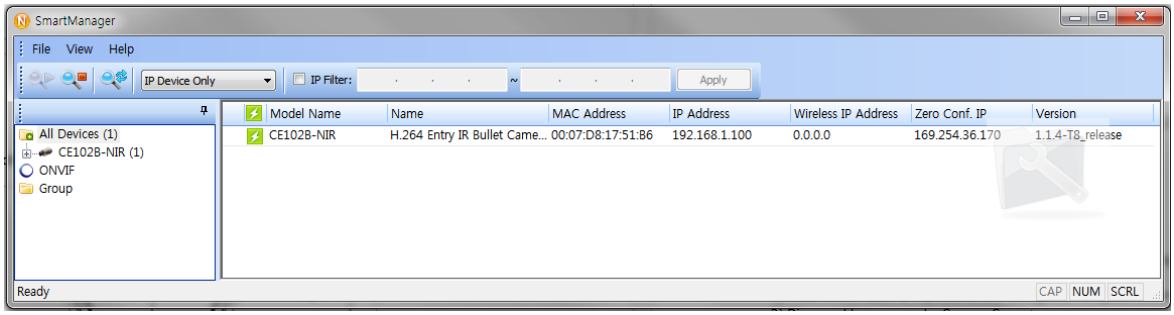
- **Connecting the Power**
  Connect the 12 VDC power adaptor (customer-supplied) to the camera.
  (This connection is not used if using PoE power.)

2.3 Network Connection and IP assignment

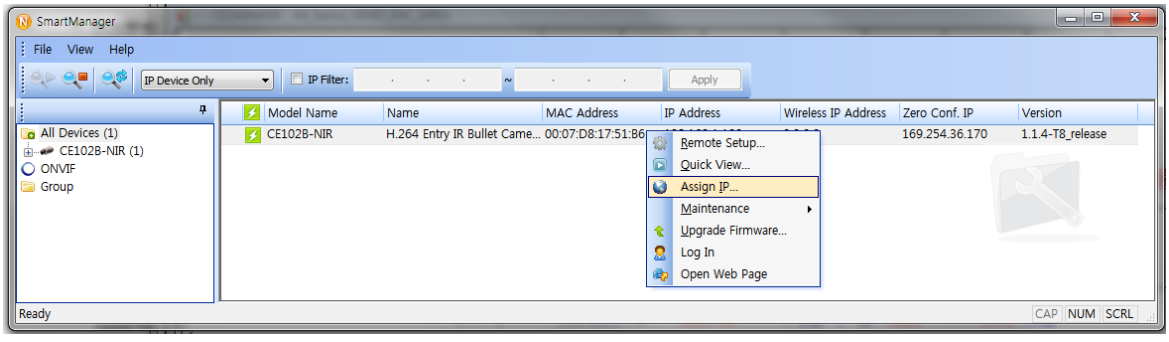
The network camera is designed for use on an Ethernet network and requires an IP address for access. Most networks today have a DHCP server that automatically assigns IP addresses to connected devices. By the factory default, your camera is set to obtain the IP address automatically via DHCP server. If your network does not have a DHCP server the network camera will use 192.168.1.100 as the default IP address.

If DHCP is enabled and the product cannot be accessed, run the “Smart Manager” utility on the CD to search and allocate an IP address to your products, or reset the product to the factory default settings and then perform the installation again.

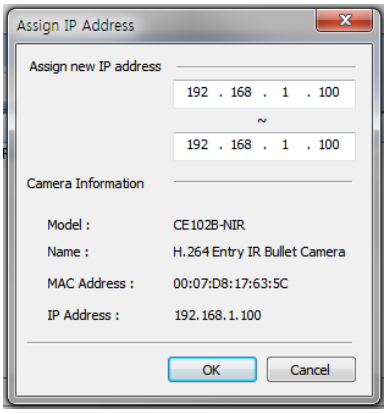
1. Connect the network camera/device to the network and power up.
2. Start SmartManager utility (Start>All programs>SmartManager>SmartManager); the main window displays. After a short while any network devices connected to the network will be displayed in the list.



3. Select the camera on the list and click right button of the mouse. The pop-up menu below displays.



4. Select Assign IP. The Assign IP window displays. Enter the required IP address.



Note: For more information, refer to the Smart Manger User’s Manual.

3. Operation

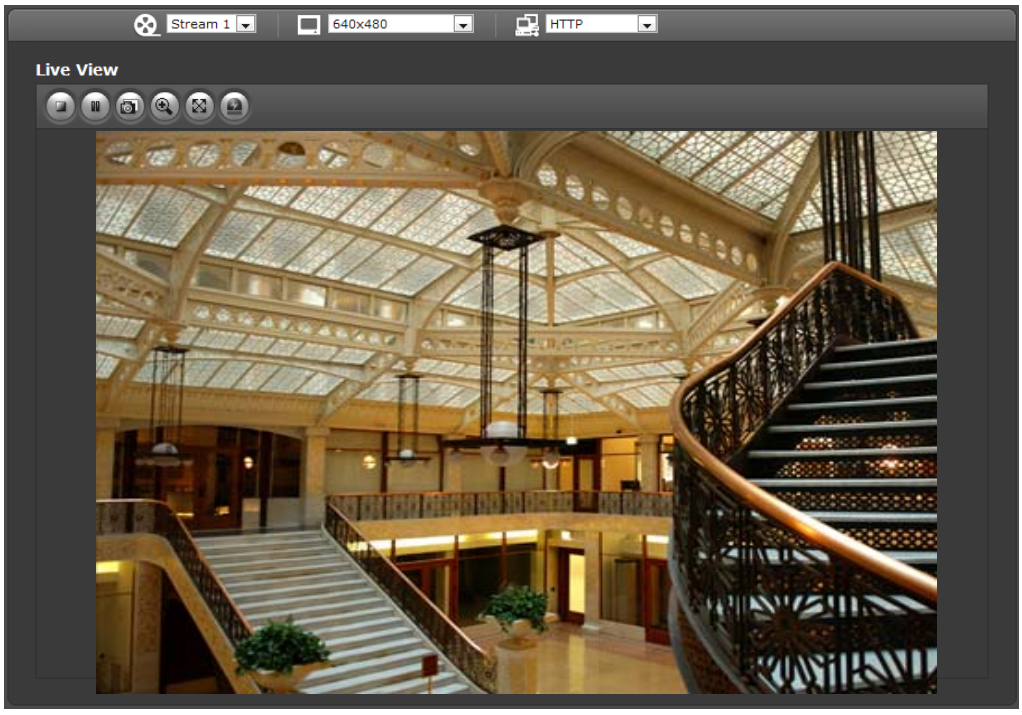
The network camera can be used with Windows® operating system and browsers. The recommended browsers are Internet Explorer®, Safari®, Firefox®, Opera® and Google® Chrome® with Windows.

Note: To view streaming video in Microsoft® Internet Explorer, set your browser to allow ActiveX controls.
Note: Some screens may appear different (i.e., color scheme) depending on the firmware version, but the functionality is the same or similar.

3.1 Access from a browser

1. Start a browser (i.e., Internet Explorer).
2. Enter the IP address or host name of the network camera in the Location/Address field of your browser.
3. You can see a starting page. Click Live View or Setup to enter web page.

4. The network camera's **Live View** page appears in your browser.



3.2. Access from the internet

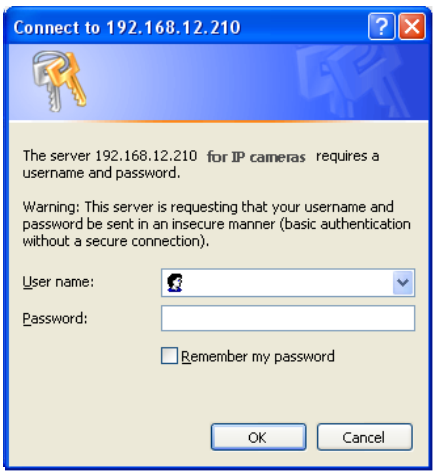
Access from the internet once connected, the Network Camera is accessible on your local network (LAN). To access the network camera from the Internet you must configure your broadband router to allow incoming data traffic to the network camera. To do this, enable the NAT-traversal feature, which will attempt to automatically configure the router to allow access to the network camera. This is enabled from Setup > System > Network > NAT.

For more information, refer to “3.5.5 System>Network>NAT” of User’s Manual.

3.3 Setting the admin password over a secure connection

To gain access to the product, the password for the default administrator user must be set. This is done in the “Admin Password” dialog, which is displayed when the network camera is accessed for the setup at the first time. Enter your admin name and password, set by the administrator.

Note: The default administrator username is “ADMIN” and password is “1234”. If the password is lost, the network camera must be reset to the factory default settings. See section “3.8 Resetting to the Factory Default Settings” for more details


Connect to 192.168.12.210
The server 192.168.12.210 for IP cameras requires a username and password.
Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).
User name:
Password:
Remember my password
OK
Cancel

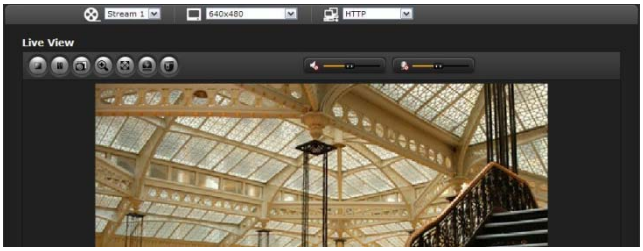
To prevent network eavesdropping when setting the admin password, use an encrypted HTTPS connection, which requires an HTTPS certificate (see note below).

To set the password via a standard HTTP connection, enter it directly in the first dialog box.
To set the password via an encrypted HTTPS connection, see “3.5.5 System >Security>HTTPS”.

Note: HTTPS (Hypertext Transfer Protocol over SSL) is a protocol used to encrypt the traffic between web browsers and servers. The HTTPS certificate controls the encrypted exchange of information.

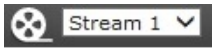
3.4 Live View Page

The live view page comes in several screen modes, for example: 1920x1080, 1280x1024, 1280x720, 800x600, 704x480 (576), 640x480, 352x240 (288) and 320x240. Select the most suitable mode in accordance with your PC specifications and monitoring purposes.



1) General controls

Live View Page Search & Playback Page Setup Page Help Page



The video drop-down list allows you to select a customized or pre-programmed video stream on the live view page. Stream profiles are configured under Setup > Basic Configuration > Video & Image. For more information, see section “3.5.1 Basic Configuration > Video & Image” of this user’s manual.

The resolution drop-down list allows the selection of the most suitable video resolution to be displayed on Live View page.

The protocol drop-down list allows you to select which combination of protocols and methods to use depends for your viewing requirements and on the properties of your network.

2) Control toolbar

The live viewer toolbar is available in the web browser page only. It displays the following buttons:

The Stop button stops the video stream being played. Pressing the key again toggles the start and stop. The Start button connects to the network camera or start playing a video stream.

The Pause button temporarily stops (pauses) the video stream being played.

The Snapshot button takes a picture (snapshot) of the current image. The location where the image is saved can be specified.

The digital zoom activates a zoom-in or zoom-out function for video image on the live screen.

The Full Screen button causes the video image to fill the entire screen area. No other windows will be visible. Press the 'Esc' button on the computer keyboard to cancel full screen view.

The Manual Trigger button activates a pop-up window to manually start or stop the event.

3) Video Streams

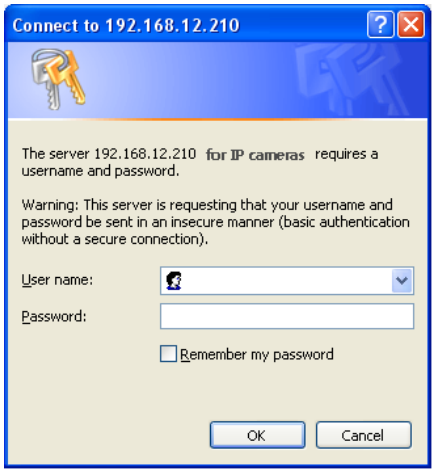
The network camera provides several images and video stream formats. Your requirements and the properties of your network will determine the type you use.

The Live View page in network camera provides access to H.264, MPEG-4 and Motion JPEG video streams, and to the list of available video streams. Other applications and clients can also access these video streams/images directly, without going via the Live View page.

3.5 Network Camera Setup

This section describes how to configure the network camera, and is intended for product Administrators, who have unrestricted access to all the Setup tools; and Operators, who have access to the settings for Basic, Live View, Video & Image and System Configuration.

You can configure the network camera by clicking Setup in the top right-hand corner of the Live View page. Click on to access the online help that explains the setup tools

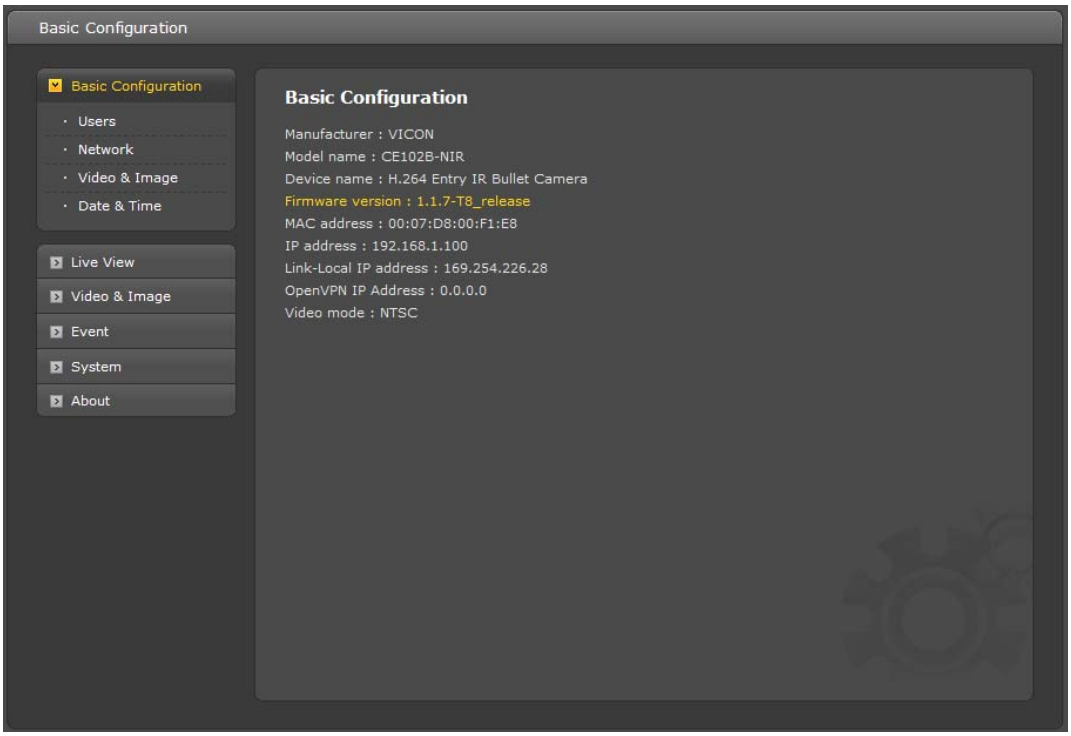

Connect to 192.168.12.210
The server 192.168.12.210 for IP cameras requires a username and password.
Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).
User name:
Password:
Remember my password
OK
Cancel

When accessing the network camera for the first time, the “Admin Password” dialog appears. Enter your admin name and password, set by the administrator.

Note: If the password is lost, the network camera must be reset to the factory default settings. See “3.8 Resetting to the Factory Default Settings”. The default administrator username is “ADMIN” and password is “1234”.

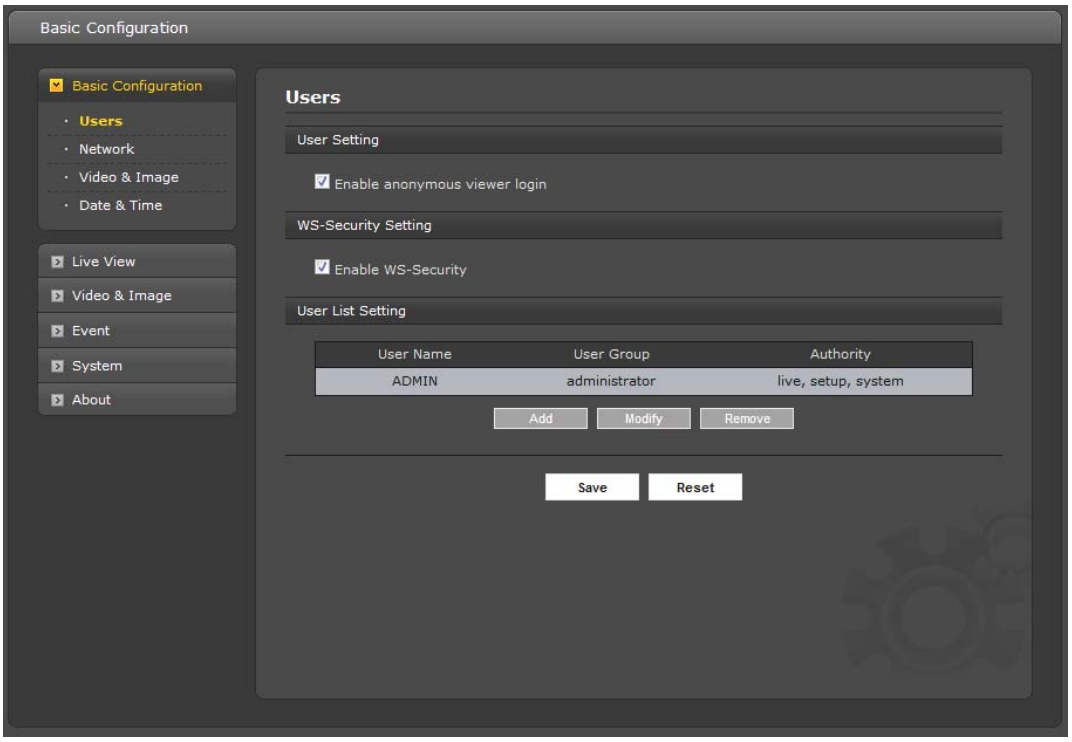
3.5.1 Basic Configuration

You can see the device information in this information page.



1) Users

User access control is enabled by default. An administrator can set up other users, by giving these user names and passwords. It is also possible to allow anonymous viewer login, which means that anybody may access the Live View page, as described below:



The **user list** displays the authorized users and user groups (levels):

User Group	Authority
Guest	Provides the lowest level of access, which only allows access to the Live View page.
Operator	An operator can view the Live View page, create and modify events, and adjust certain other settings. Operators have no access to System Options.
Administrator	An administrator has unrestricted access to the Setup tools and can determine the registration of all other users.

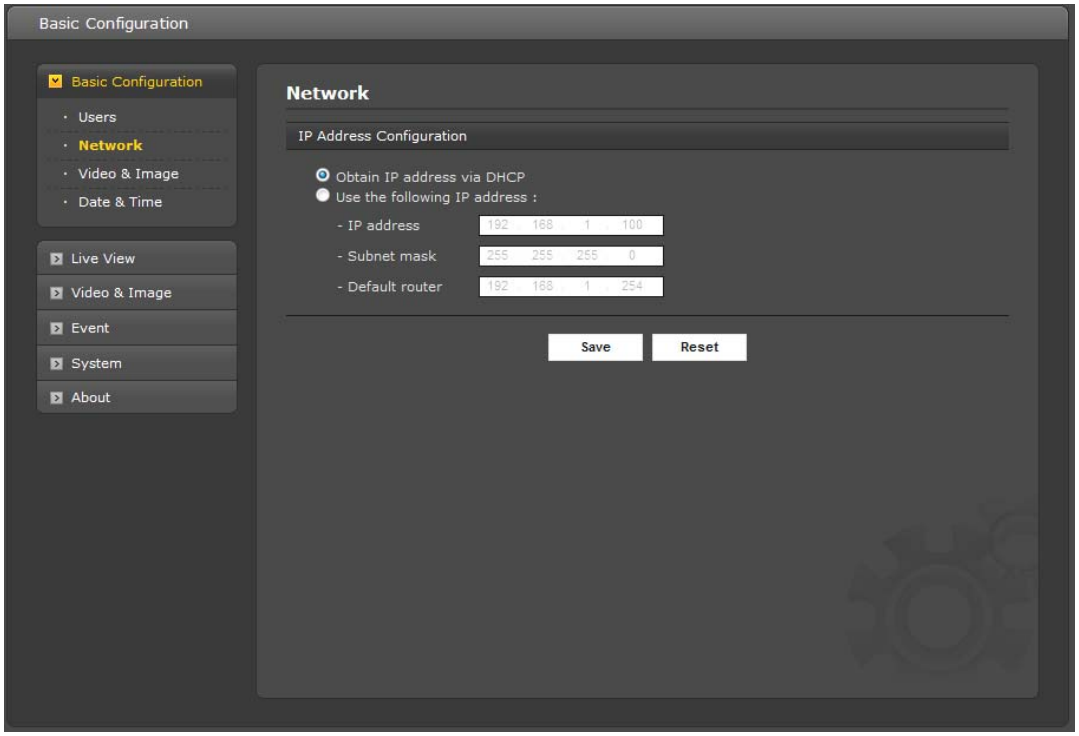
- **Enable anonymous viewer login:** Check the box to use the webcasting features. Refer to "3.5.3 Video & Image" for more details.

- **Enable WS-Security:** Do not check this box to connect and monitor the network camera through Vicon's viewing software using drivers older than 935.

  Note: WS-Security is an open format for signing and encryption of message parts, for supplying credentials in the form of security tokens, and for security passing those tokens in a message.

2) Network

The network camera supports both IP version 4 and IP version 6. Both versions may be enabled simultaneously, and at least one version must always be enabled. When using IPv4, the IP address for the network camera can be set automatically via DHCP, or a static IP address can be set manually. If IPv6 is enabled, the network camera receives an IP address according to the configuration in the network router. There is also the option of using the Internet Dynamic DNS Service. For more information on setting the Network, please see Setup> System>Security>Network.



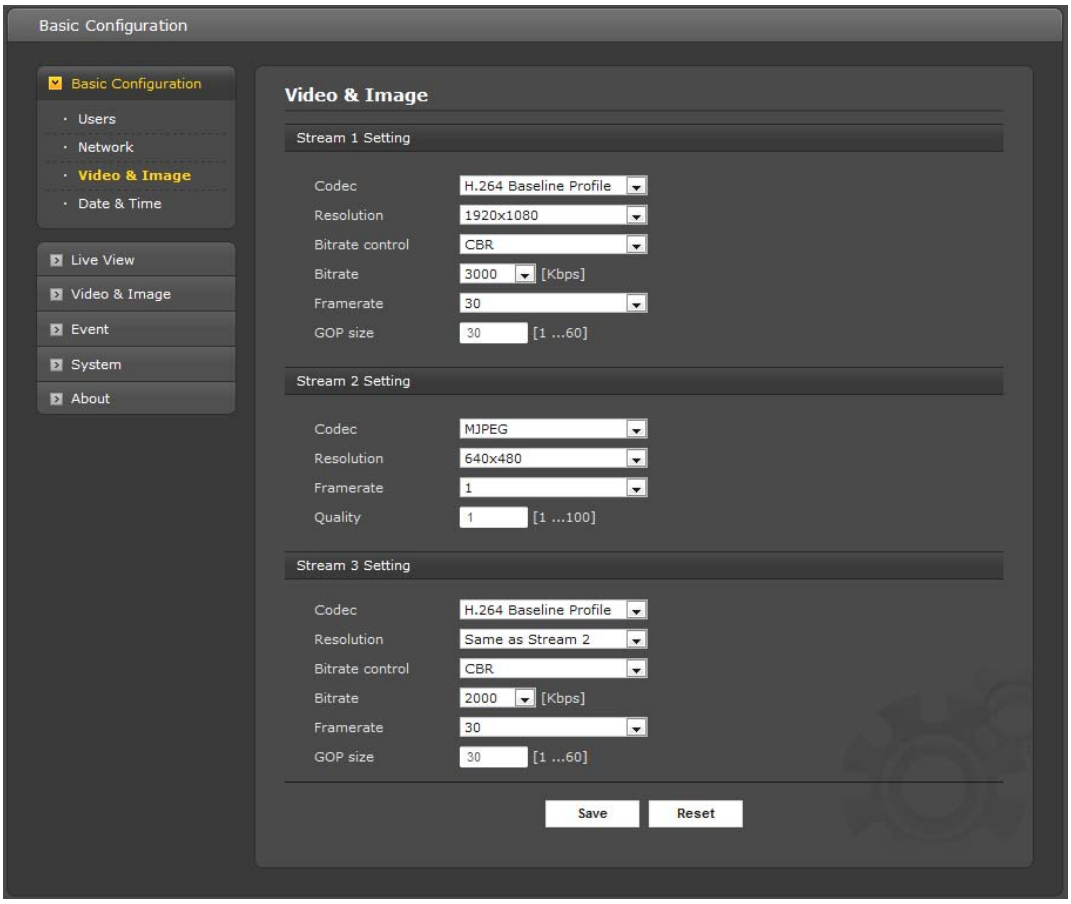
- **Obtain IP address via DHCP** - Dynamic Host Configuration Protocol (DHCP) is a protocol that lets network administrators centrally manage and automate the assignment of IP addresses on a network. DHCP is enabled by default. Although a DHCP server is mostly used to set an IP address dynamically, it is also possible to use it to set a static, known IP address for a particular MAC address.

- **Use the following IP address** - To use a static IP address for the network camera, check the radio button and then make the following settings:
  - **IP address** - Specify a unique IP address for your network camera.
  - **Subnet mask** - Specify the mask for the subnet the network camera is located on.
  - **Default router** - Specify the IP address of the default router (gateway) used for connecting devices attached to different networks and network segments.

Notes:

1. DHCP should only be enabled if using dynamic IP address notification, or if your DHCP server can update a DNS server, which then allows you to access the network camera by name (host name). If DHCP is enabled and you cannot access the unit, you may have to reset it to the factory default settings and then perform the installation again.
2. The ARP/Ping service is automatically disabled two minutes after the unit is started, or as soon as an IP address is set.
3. Pinging the unit is still possible when this service is disabled.

3) Video & Image



- **Stream1 Setting**
  - **Codec:**

    The codec settings are separated into MPEG4 and H.264.

    H.264 is also known as MPEG-4 Part 10. This is the new generation compression standard for digital video. This function offers higher video resolution than Motion JPEG or MPEG-4 at the same bit rate and bandwidth, or the same quality video at a lower bit rate.

    There are 4 pre-programmed stream profiles available for quick set-up.
    Choose the form of video encoding you wish to use from the drop-down list:

    * **H.264 HP (High Profile):** The primary profile for broadcast and disc storage applications, particularly for high-definition television applications (for example, this is the profile adopted by the Blu-ray Disc storage format and the DVB HDTV broadcast service).
    * **H.264 MP (Main Profile):**
      Primarily for low-cost applications that require additional error robustness, this profile is used rarely in videoconferencing and mobile applications; it does add additional error resilience tools to the Constrained Baseline Profile. The importance of this profile is fading after the Constrained Baseline Profile has been defined.
    * **H.264 BP (Baseline Profile):**
      Originally intended as the mainstream consumer profile for broadcast and storage applications, the importance of this profile faded when the High profile was developed for those applications.

* **MPEG4 SP (Simple Profile):**
Mostly aimed for use in situations where low bit rate and low resolution are mandated by other conditions of the applications, like network bandwidth, device size, etc.

- **Resolution:**
Resolution enables users to determine a basic screen size when having an access through the Web Browser or PC program. The screen size control comes in several modes, such as 1920x1080, 1280x1024, 1280x720, 800x600, 704x480 (576), 640x480, 352x240 (288) and 320x240. Users can reset the selected screen size anytime while monitoring the screen on a real-time basis.

- **Bitrate control:**
The bit rate can be set as Variable Bit Rate (VBR) or Constant Bit Rate (CBR). VBR adjusts the bit rate according to the image complexity, using up bandwidth for increased activity in the image, and less for lower activity in the monitored area.

CBR allows you to set a fixed target bitrate that consumes a predictable amount of bandwidth. As the bit rate would usually need to increase for increased image activity, but in this case cannot, the frame rate and image quality are affected negatively. To partly compensate for this, it is possible to prioritize either the frame rate or the image quality whenever the bit rate needs to be increased. Not setting a priority means the frame rate and image quality are equally affected.

- **Bitrate:**
When it is necessary to adjust a smooth transmission status according to network situations, users can increase the compressibility to carry out the network transmission stably. Alternatively, when it is necessary to maintain a detailed monitoring screen by enhancing the image quality, users can do so by decreasing the compressibility. In each case, adjust this function according to the network status and monitoring purposes. The default is 2000 (Kbps).

- **Frame rate:**
Upon the real-time play, users should select a frame refresh rate per second. If the rate is high, the image will become smooth. On the other hand, if the rate is low, the image will not be natural but it can reduce a network load.

- **GOP size:**
Select the GOP (Group of Picture) size. If users want to have a high quality of fast image one by one, decrease the value. For the purpose of general monitoring, do not change a basic value. Such act may cause a problem to the system performance. Vicon recommends that GOP be the same as the fps.

- **Stream2 Setting**
  Sometimes the image size is large due to low light or complex scenery. Adjusting the frame rate and quality help to control the bandwidth and storage used by the Motion JPEG video stream in these situations. Limiting the frame rate and quality optimizes bandwidth and storage usage, but may give poor image quality. To prevent increased bandwidth and storage usage, the Resolution, Frame rate, and Frame Quality should be set to an optimal value.

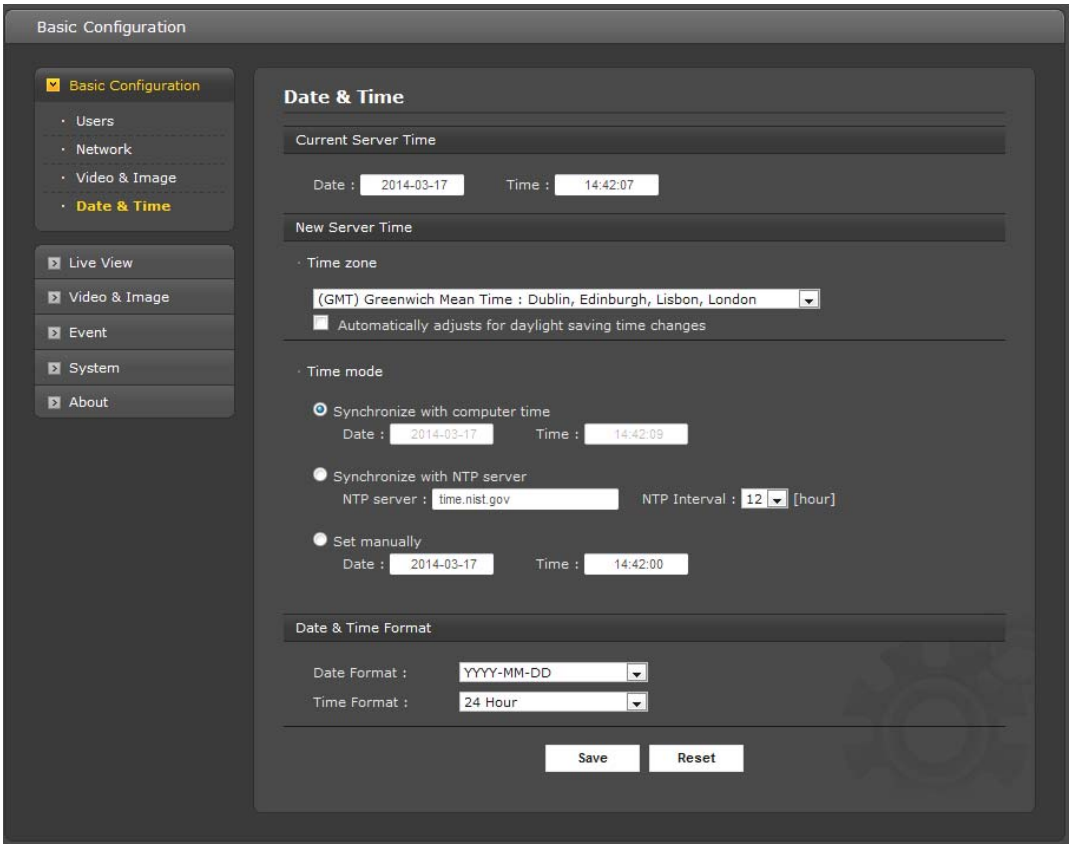
  - **JPEG resolution:** Same as the Stream1 Resolution Setting.
  - **JPEG frame rate:** Same as the Stream1 Framerate Setting.

  - **JPEG quality:**
    Select the picture quality. If users want to have a high quality of fast image one by one, please decrease the value. For the purpose of general monitoring, please do not change a basic value. Such act may cause a problem to the system performance.

- **Stream3 Setting**
  Use the same as the Stream1 settings.

When satisfied with the settings, click **Save**, or click **Reset** to revert to previously saved settings.

4) Date & Time



- **Current Server Time**
  This displays the current date and time (24h clock). The time can be displayed in 12h clock format (see below).

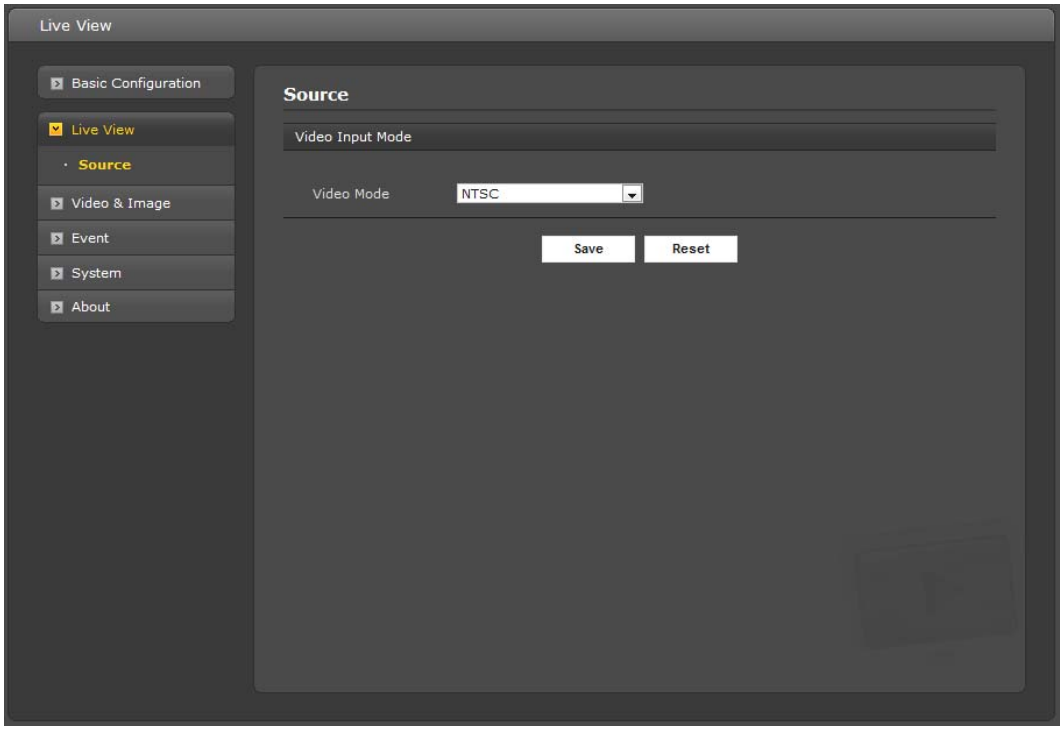
- **New Server Time**
  Select your time zone from the drop-down list. If you want the server clock to automatically adjust for daylight savings time, select the “Automatically adjusts for daylight saving time changes”.

  From the **Time Mode** section, select the preferred method to use for setting the time:
  - **Synchronize with computer time:** sets the time from the clock on your computer.
  - **Synchronize with NTP Server:** the network camera will obtain the time from an NTP server every 60 minutes.
  - **Set manually:** this option allows you to manually set the time and date.
- **Date & Time Format**
  Specify the formats for the date and time (12h or 24h) displayed in the video streams.
  Select Date & Time format from the drop-down list.
  - **Date Format:** Specify the date format. YYYY: Year, MM: Month, DD: Day
  - **Time Format:** Specify the date format. 24Hours or 12 Hours

When the settings are complete, click **Save**, or click **Reset** to revert to previously saved settings.

3.5.2 Live View

▼ Source

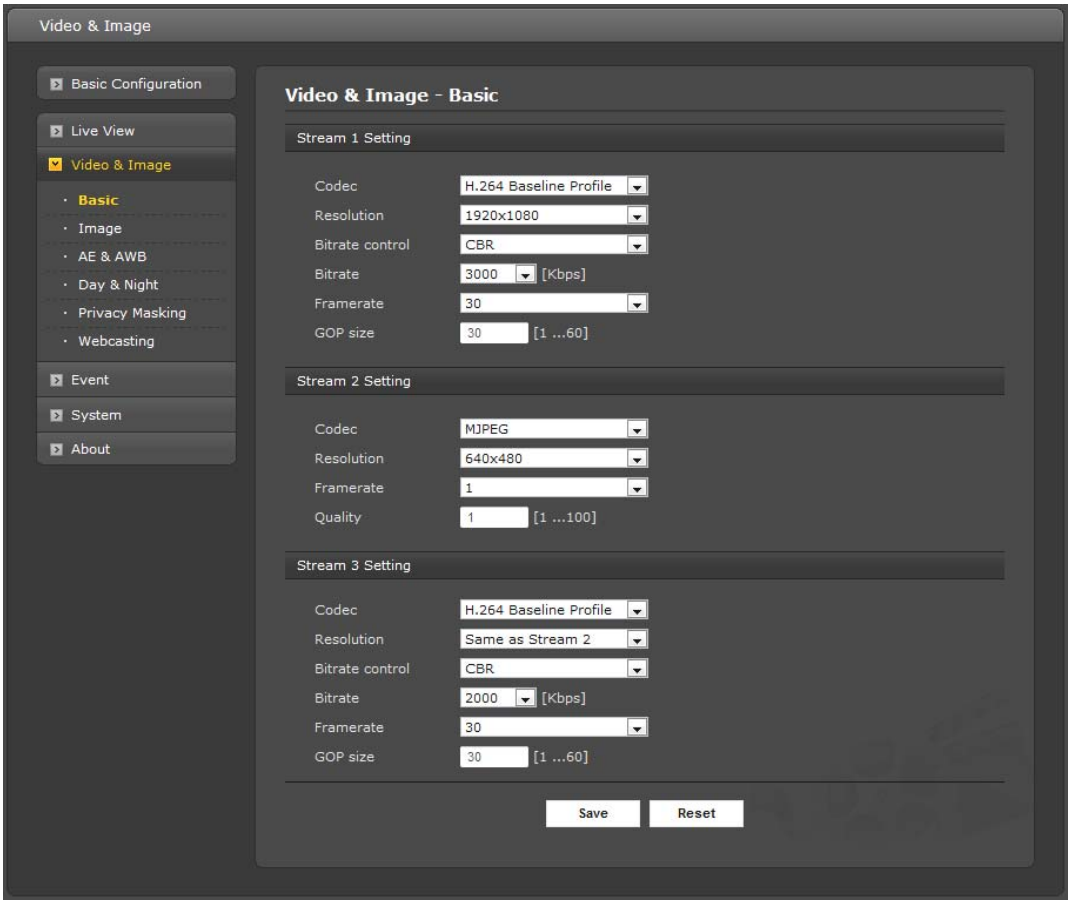


Use the Video Mode drop-down list to select the video input mode, NTSC or PAL. This defines the Video Output Port for the Service Monitor.

When the settings are complete, click **Save**, or click **Reset** to revert to previously saved settings.

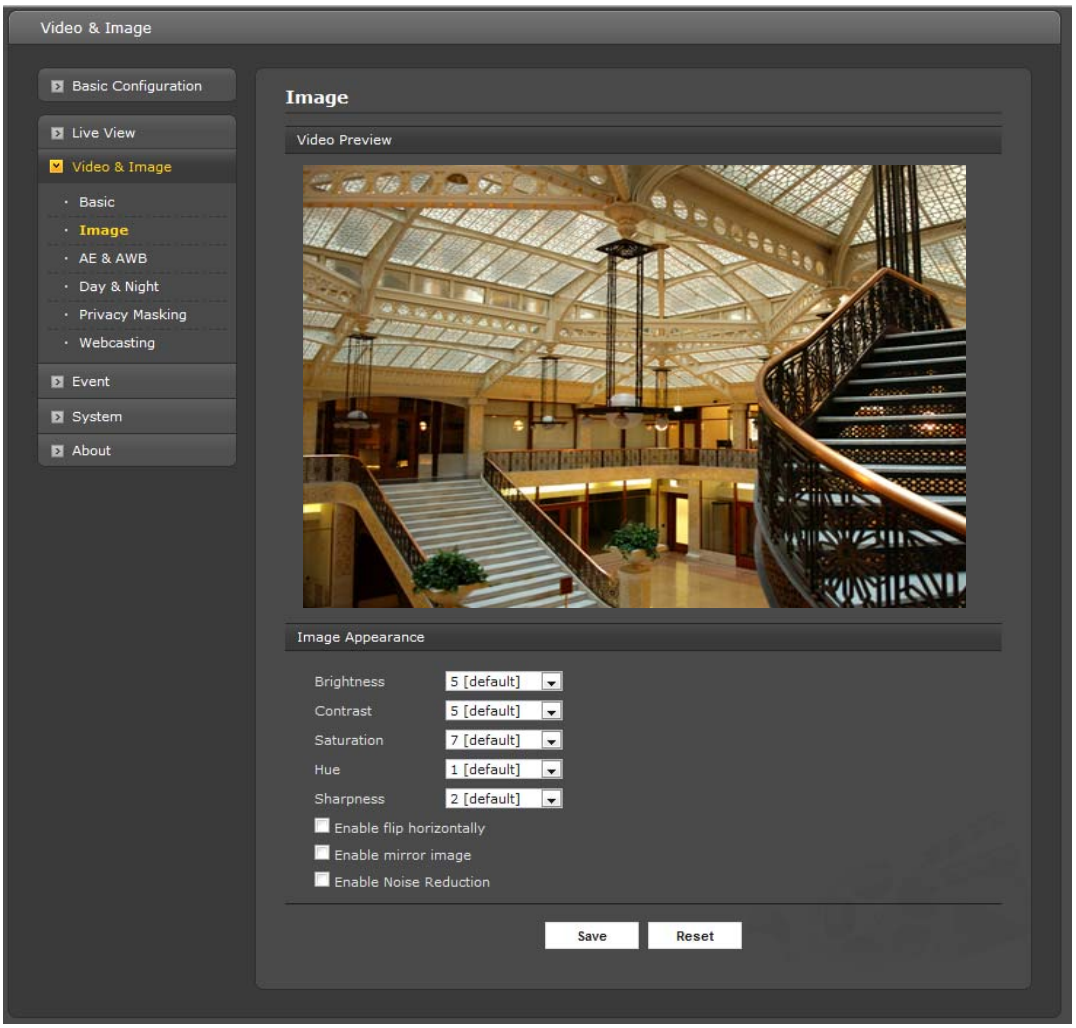
3.5.3 Video & Image

▼ Basic



Refer to “3.5.1 Basic Configuration > Video & Image” for more details.

▼ Image



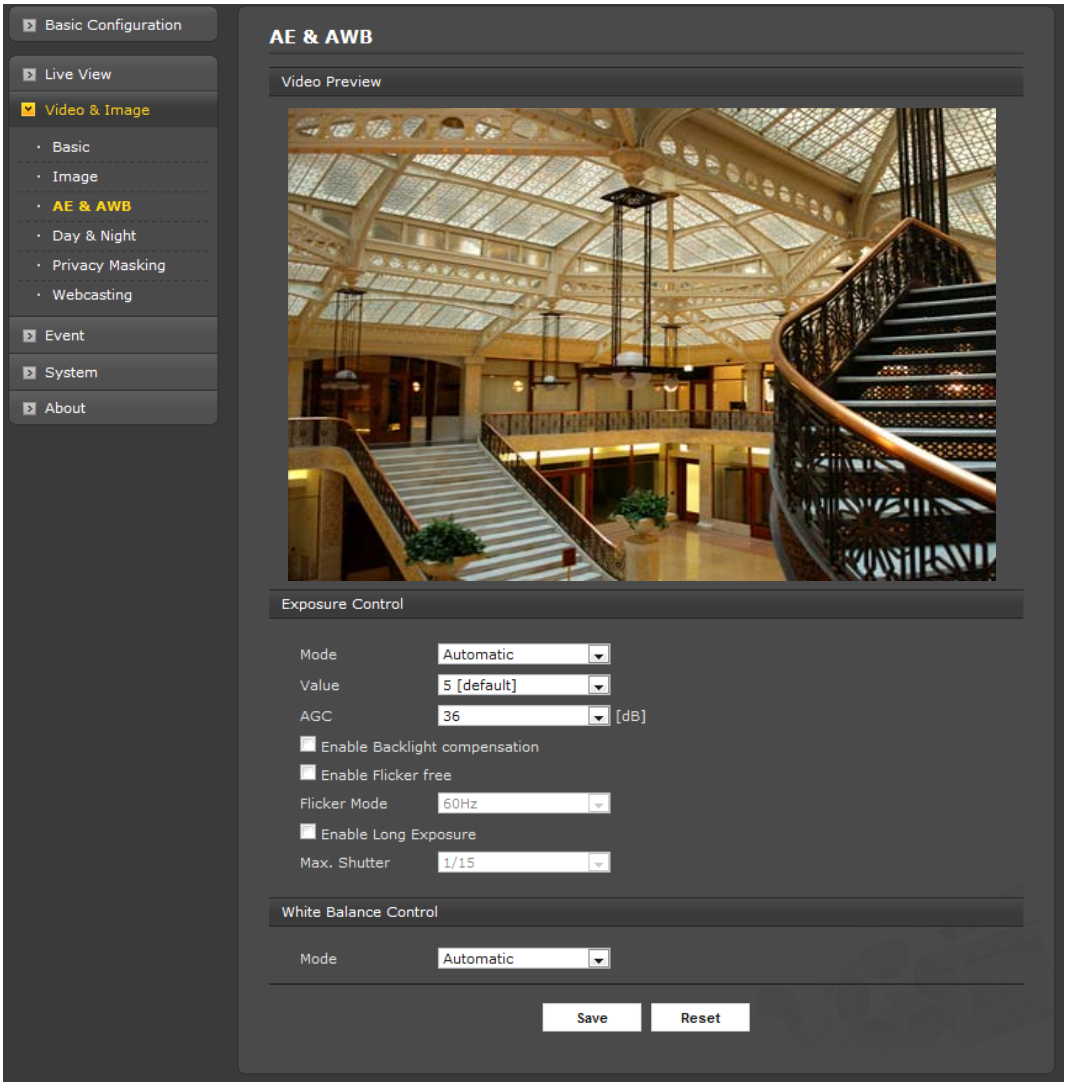
- **Image Appearance**

  This page provides access to the advanced image settings for the network camera.

  - **Brightness:** The image brightness can be adjusted in the range 1-10, where a higher value produces a brighter image.
  - **Contrast:** Adjust the image's contrast by raising or lowering the value in this field, 1-10.
  - **Saturation:** Select an appropriate level by entering a value in the range 1-10. Lower values mean less color saturation.
  - **Hue:** Select an appropriate level by entering a value in the range 1-10.
  - **Sharpness:** Controls the amount of sharpening applied to the image. A sharper image might increase image noise, especially in low light conditions. A lower setting reduces image noise, but the image would be less sharp.
  - **Enable flip image:** Check this box to flip the image.
  - **Enable mirror image:** Check this box to mirror the image.
  - **Enable Noise Reduction:** Check this box to reduce an image noise.

When the settings are complete, click **Save**, or click **Reset** to revert to previously saved settings.

▼ AE & AWB



- **Exposure control**

This page provides access to set the exposure and white balance of the network camera.

- **Mode:** Supports exposure modes to control the amount of light detected by the camera sensor based on settings for light conditions. The default setting is Auto mode.
  * **Automatic:** Automatically sets the amount of light detected by the image sensor.
  * **Hold Current:** Fixes the exposure at its current state.
- **Value:** Select a value in the drop-down list to tune the exposure. The default setting is 5.
- **AGC:** Select a value in the drop-down list to specify the level according to the screen luminance. The default setting is 30dB.
- **Enable Backlight Compensation:** Set this checkbox to activate the BLC operation.
- **Enable Flicker free:** Set this checkbox to activate the flicker free operation.
- **Flicker Mode** - Provides the options for flicker.
  * **50Hz:** Select at 50 Hz environments.
  * **60Hz:** Select at 60 Hz environments.
- **Enable Long Exposure:** Set this checkbox to activate the electronic shutter of the camera.
  * **Max. Shutter:** Select a shutter speed value in the drop-down list. The default setting is 1/15.

- **White Balance Control**

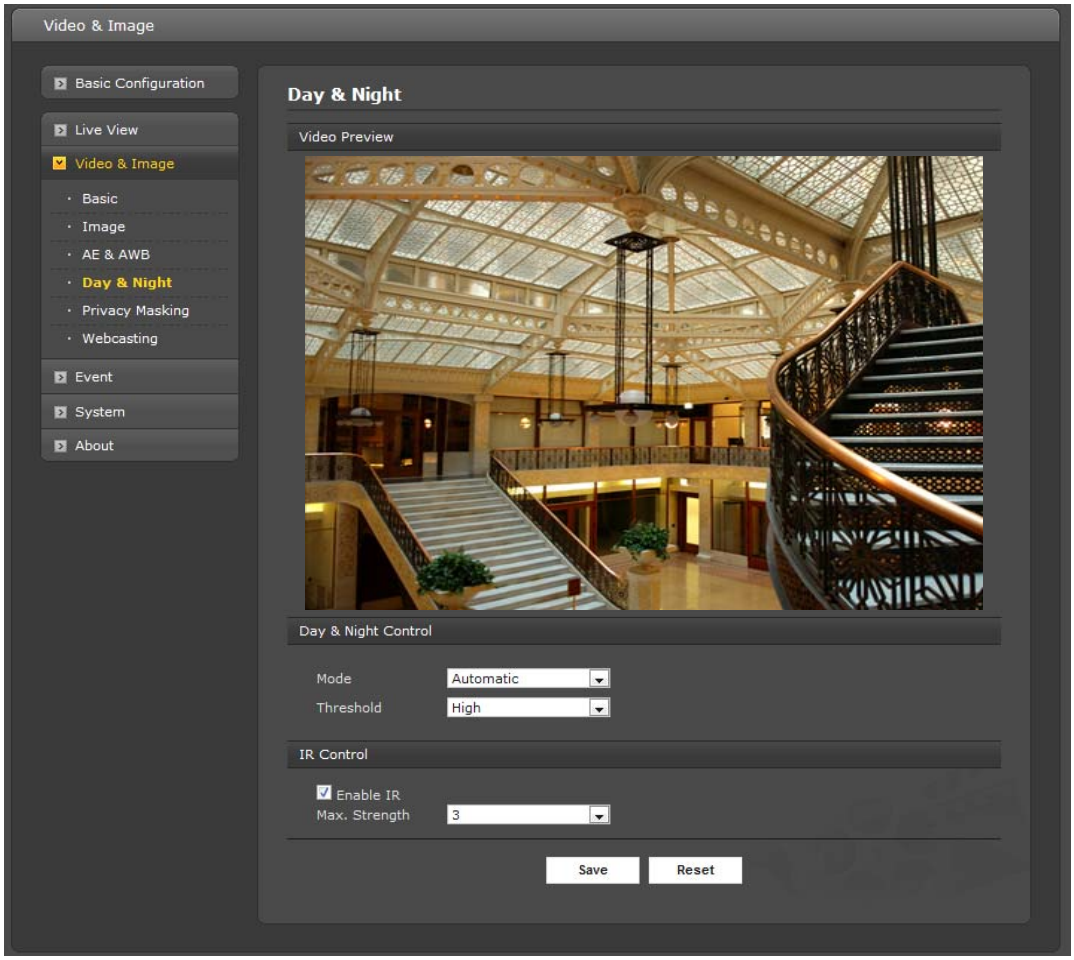
  This adjusts the relative amount of red, green and blue primary colors in the image so that the neutral colors are reproduced correctly. The camera can be set to automatically adjust for the type of light and compensate for its color. Alternatively, the type of light source can be set manually.

  From the drop-down list, select the white balance setting suitable for the lighting used for your camera. The available options are:

  - **Automatic:** Automatic identification and compensation for the light source color. This can be used in most situations and is the recommended setting.
  - **Fixed Incandescent:** Fixed color adjustment, ideal for a room with incandescent (glowing) lighting and good for a normal color temperature around 2600K.
  - **Fixed Fluorescent:** Fixed color adjustment; good for fluorescent lighting with a color temperature around 4000K to 5000K.
  - **Fixed Outdoor:** Fixed color adjustment for sunny environment, with a color temperature around 6500K to 7500K.
  -

When the settings are complete, click **Save**, or click **Reset** to revert to previously saved settings.

▼ Day & Night



- **Day & Night Control**

  - **Mode:** Select the day/night mode from among three modes.
  * **Automatic:** Normally works in day mode; switches automatically to night mode in a dark place.
  * **Day:** Always works in day mode.
  * **Night:** Always works in night mode.
  - **Threshold**: Controls the how fast the change is from day to night or night to day.
  - ***High:** Quickly changes to day mode, but slowly changes to night mode.
  - ***Low:** Quickly changes to night mode, but slowly changes to day mode.

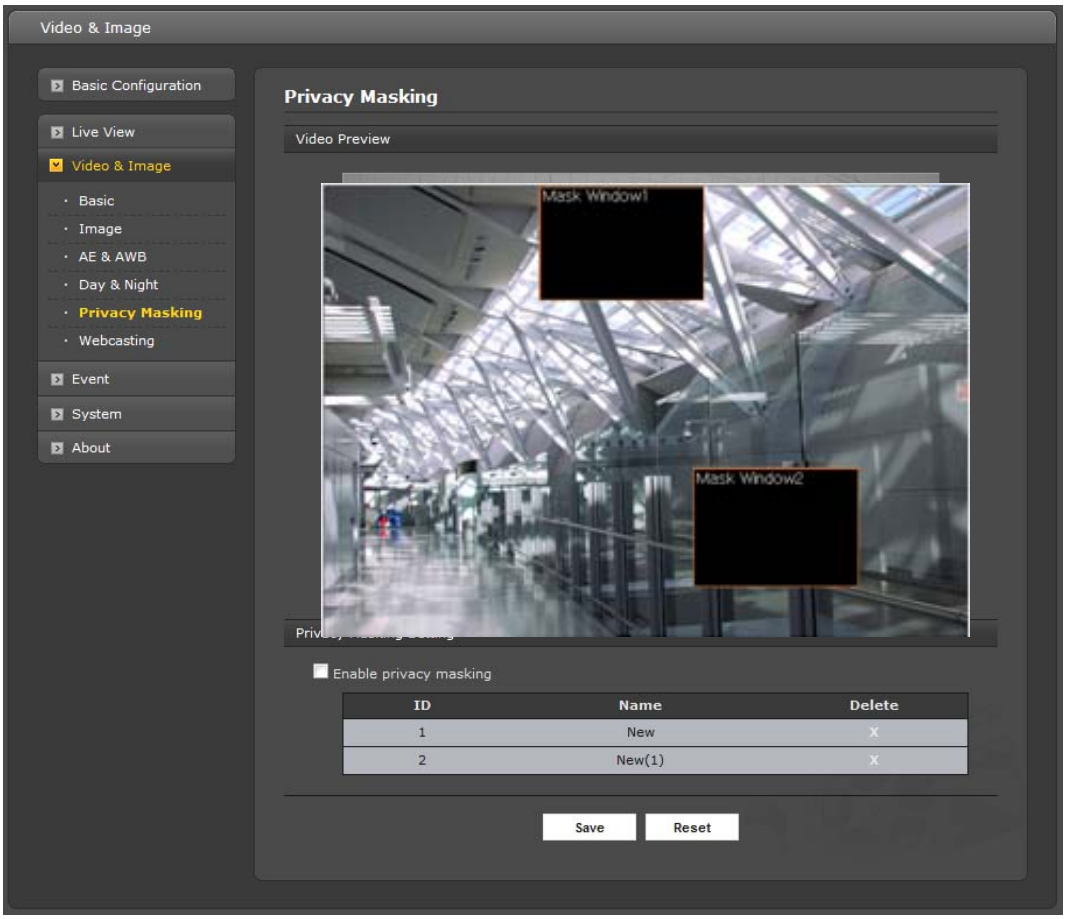
- **IR Control**

  - **Enable IR:** Check this box to activate IR operation.
  * **Max Strength:** Select a value in the drop-down list to tune the strength. The default setting is 5.

When the settings are complete, click **Save**, or click **Reset** to revert to previously saved settings.

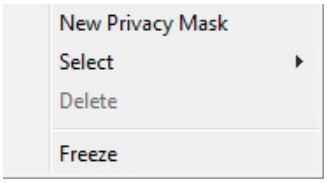
▼ Privacy Masking

The privacy masking function allows selected parts of the video image being transmitted to be masked from view. Up to eight privacy masks (or motion detection windows) can be set; the color of privacy masks is black.



Select “Enable privacy masking” to activate the privacy masking function.

The privacy masks are configured by Mask windows. Each window can be selected by clicking with the mouse. It is also possible to resize, **resize**, **delete** or **move** the window, by selecting the appropriate window at the mouse menu on the video screen.



To create a mask window, follow steps:

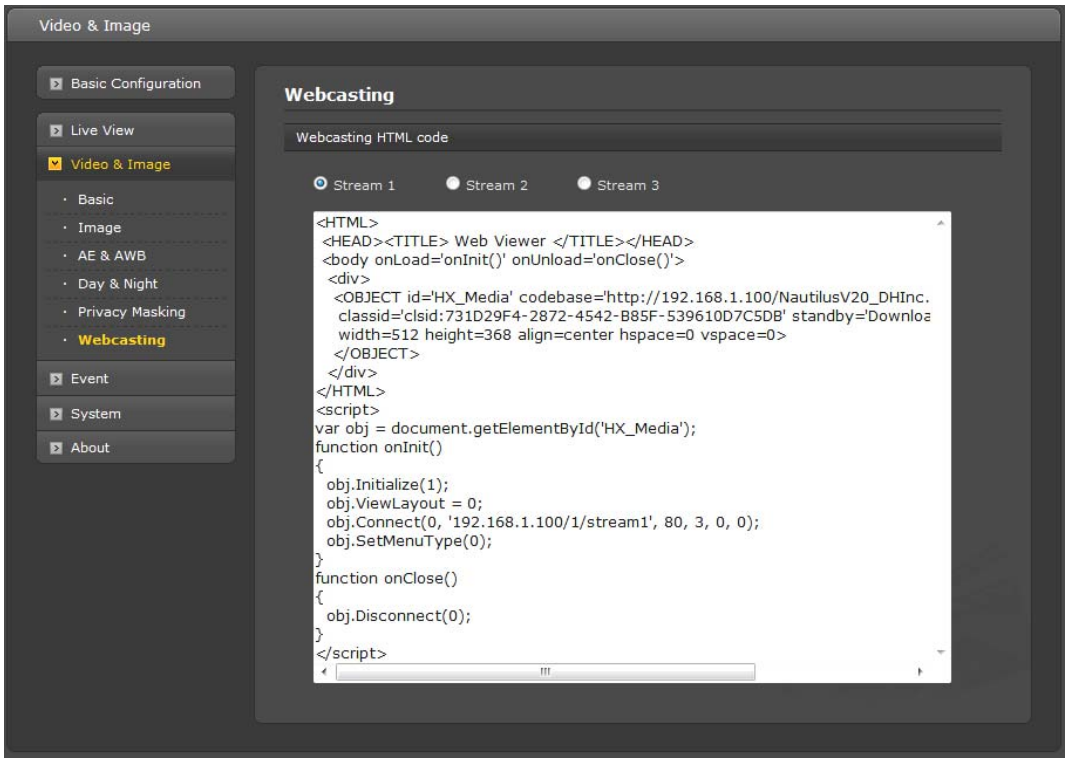
1. Click the right button of mouse to see the mouse menu.
2. Select New Privacy Mask in the mouse menu.
3. Click and drag mouse to designate a mask window area.

A mask window name can also be modified or deleted. Select a name and then modify it in the Name field or click the X in the delete column to delete. Change the size of the mask by dragging the borders or corners of the mask or click in the center of the mask to change the location; select delete button to completely remove the mask.

When the settings are complete, click **Save**, or click **Reset** to revert to previously saved settings.

▼ Webcasting

The network camera can stream live video to a website. Copy the HTML code generated on the screen and paste it in page code of the website you want to display live video.

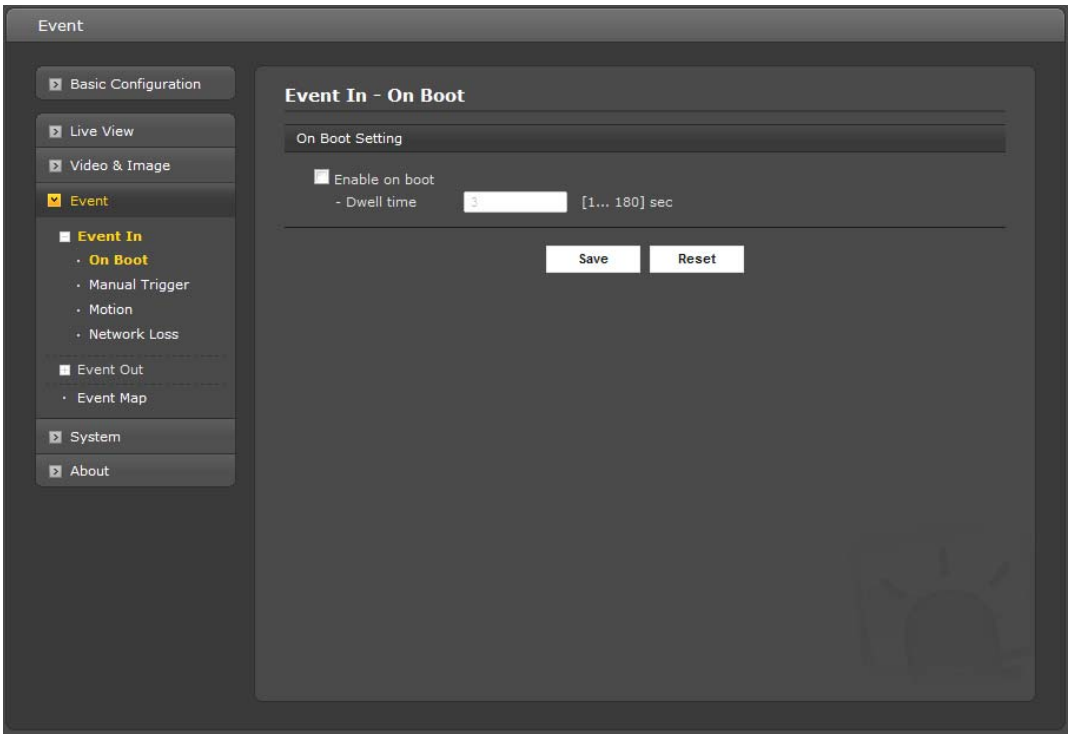


Note: To use webcasting service, the Enable Anonymous viewer login option must be checked. Refer to “3.5.1 Basic Configuration > Users” for more details.

3.5.4 Event

1) Event-In

▼ On Boot

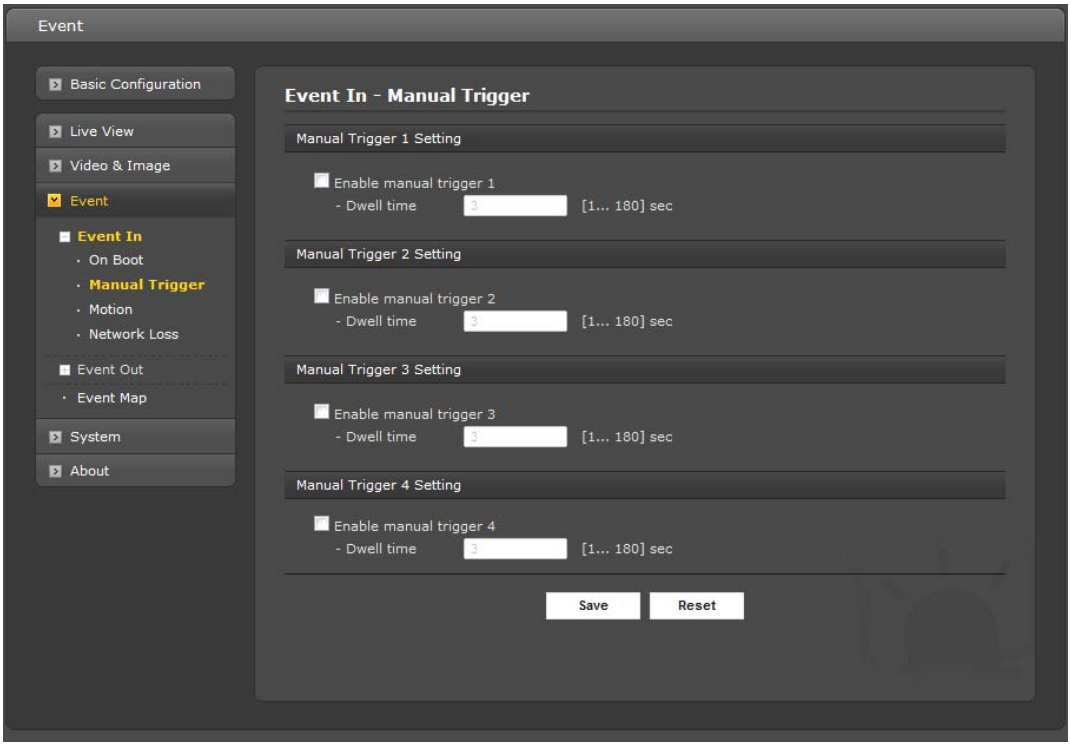


This is used to trigger the event every time the network camera is started. Select “Enable on boot” to activate the motion event.

Enter the Dwell time the event lasts from the point of detection, 1-180 seconds.

When the settings are complete, click **Save**, or click **Reset** to revert to previously saved settings.

▼ Manual Trigger



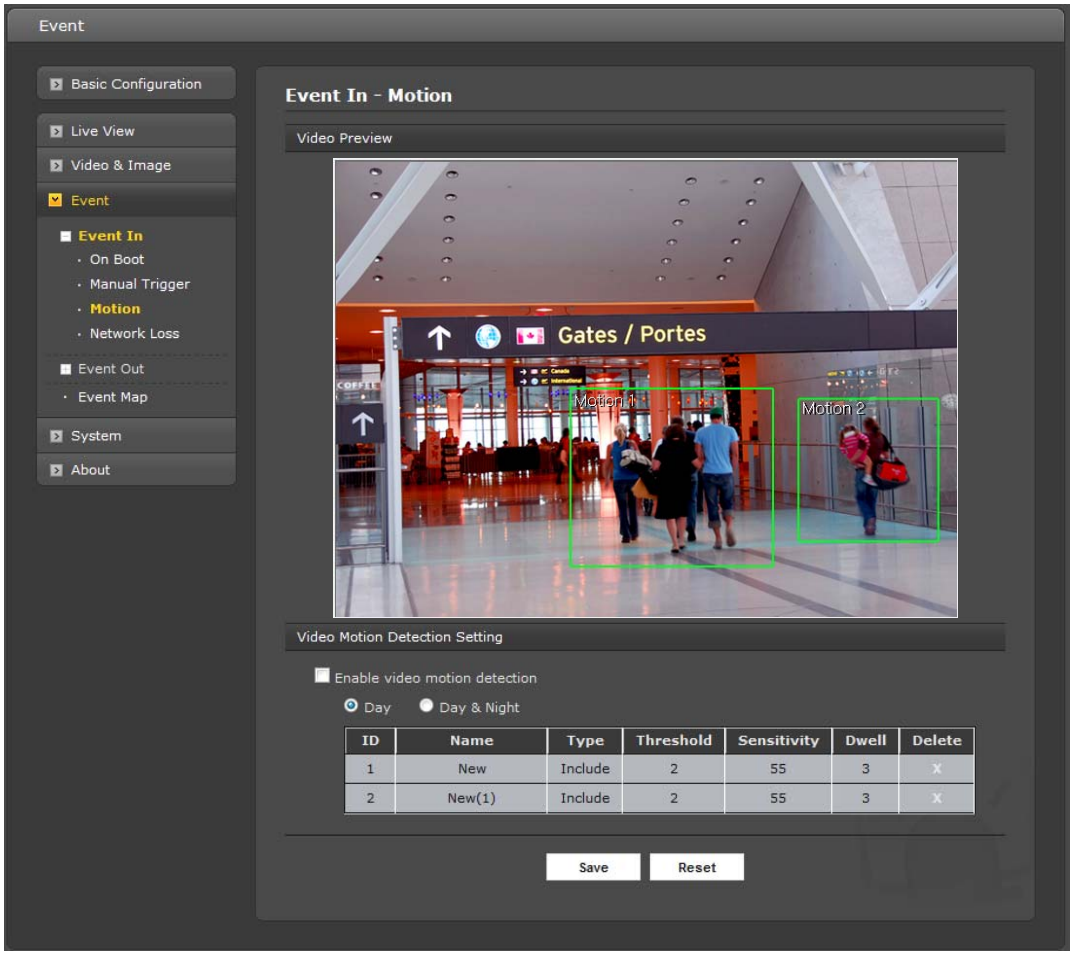
This option makes use of the manual trigger button provided on the Live View page, which is used to start or stop the event type manually. Alternatively, the event can be triggered via the product's API (Application Programming Interface).

Select “Enable manual trigger” to activate the manual trigger (for up to 4 manual triggers).

Set the dwell time the trigger lasts.

When the settings are complete, click **Save**, or click **Reset** to revert to previously saved settings.

▼ Motion



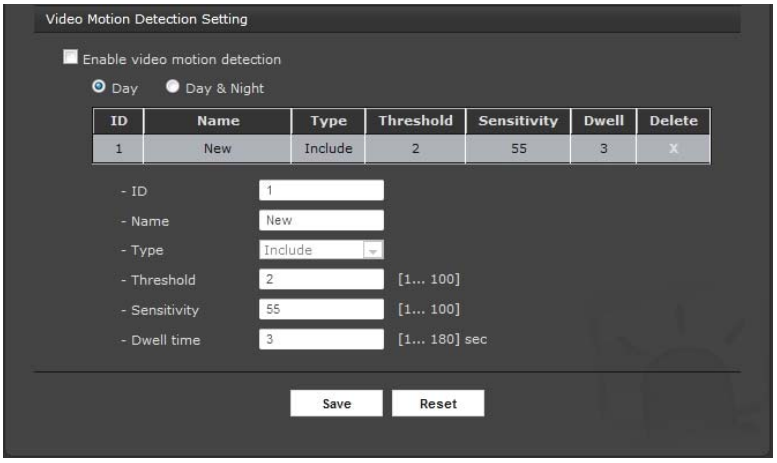
Motion detection is used to generate an alarm whenever movement occurs (or stops) in the video image. A total of 8 Motion and/or Mask windows can be created and configured.

Motion is detected in defined **Motion** windows, which are placed in the video image to target specific areas. Movement in the areas outside the motion windows will be ignored. If part of a motion window needs to be masked, this can be configured in a **Mask** window.

- **Pre-Viewer**
  Motion detection windows are configured by Motion or Mask windows. Each window can be selected by clicking with the mouse. It is also possible to **resize**, **delete** or **move** the window, by selecting the appropriate window with the mouse menu on the video screen.

To create a motion or mask window, follow steps:

1. Click the right button of mouse to see the mouse menu.
2. Select New Motion (or Mask) Window in the mouse menu.
3. Click and drag mouse to designate a motion area.



- **Motion Detection Setting**

The behavior for each window is defined by adjusting the Threshold and Sensitivity, as described below. The combination of these parameters defines whether motion has occurred; motion detection frequency is increased with a high sensitivity and a low threshold.

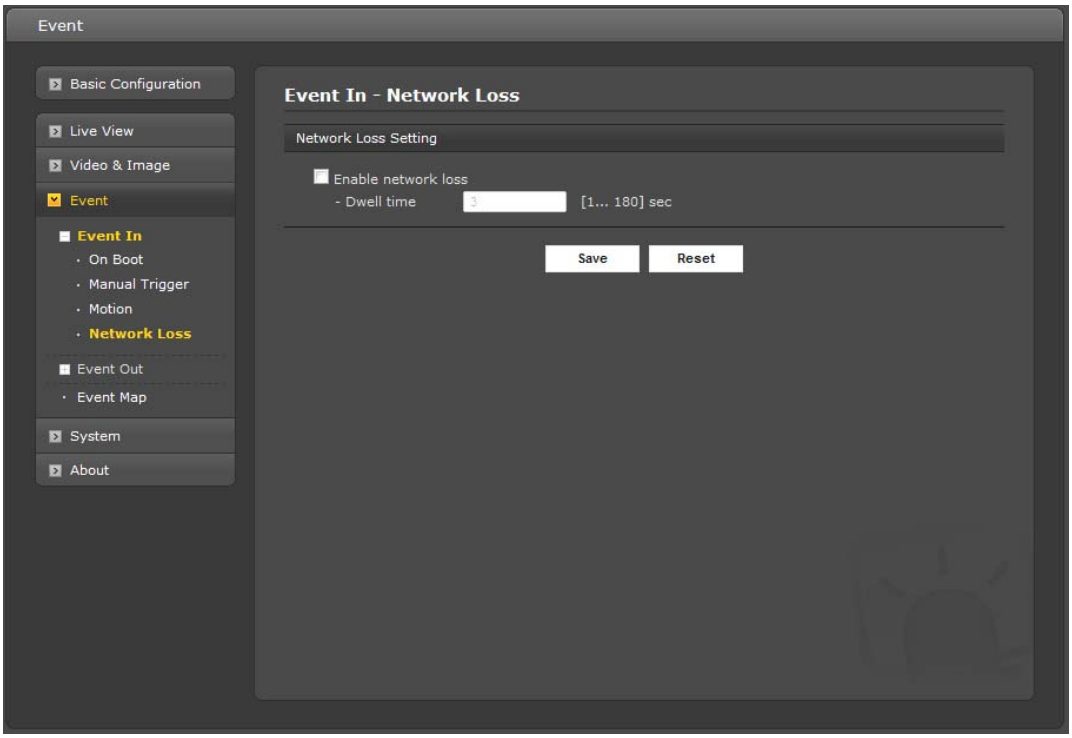
A motion index is a set of parameters describing Window Name, Type, Threshold, Sensitivity, and Dwell Time. Window Type is Include at the Motion, and Exclude at the Mask window.

- **Threshold:** Sets up the threshold for the motion detection. Threshold judges the amount of change in the area. Select from 1-100; a lower number increase frequency of alarms.
- **Sensitivity:** Sets up the sensitivity for the motion detection. Sensitivity measures the level of motion in each motion area. Select from 1-100, 1 being the least sensitive to alarm condition.
- **Dwell Time:** Set the hold time an event lasts from the point of detection of a motion (hold time).

You can also modify or delete a motion index. It can be deleted using the table and modified by selecting it and changing parameters in the table. Change the size of the mask by dragging the borders or corners of the mask or click in the center of the mask to change the location; select delete button to completely remove the mask. When the settings are complete, click **Save**, or click **Reset** to revert to previously saved settings.

To exclude parts of the Include window, select the New Mask at the mouse menu and position the Mask window as required.

▼ Network Loss

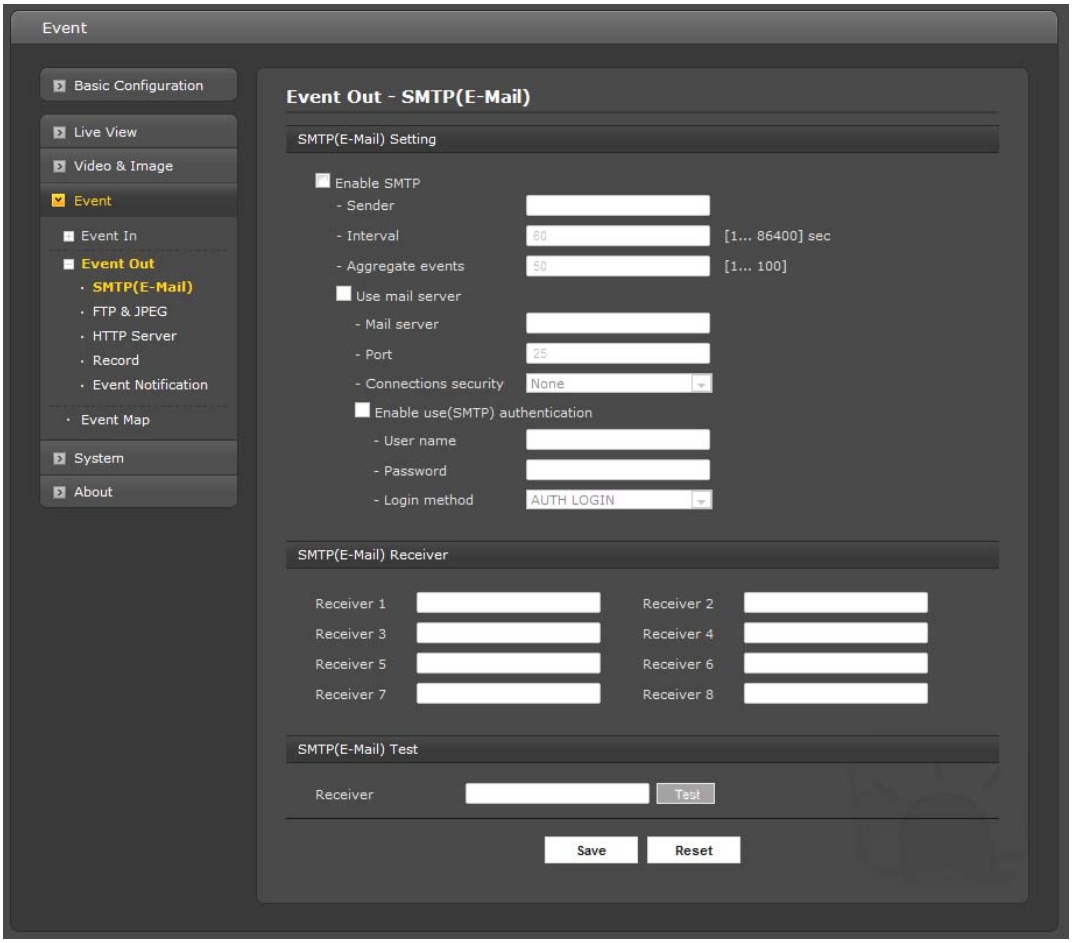


This is used to trigger the event every time the network connection is failed. Select “Enable network loss” to activate the Network Loss event. Select a dwell time for how long the event will last from the point of detection.

When the settings are complete, click **Save**, or click **Reset** to revert to previously saved settings.

2) Event-Out

▼ SMTP (E-Mail)



The network camera can be configured to send event and error email messages via SMTP (Simple Mail Transfer Protocol).

Select “Enable SMTP” to activate the SMTP operation.

- **Sender:** Enter the email address to be used as the sender for all messages sent by the network camera.
- **Interval:** Represents the frequency of the email notification when an event occurs.
- **Aggregate events:** Shows the maximum number of emails sent within each interval.

Check the box to "Use mail server" if required.

- **Mail Server/Port:** Enter the host names (or IP addresses) and port numbers for your mail server in the fields provided, to enable the sending of notifications and image email messages from the camera to predefined addresses via SMTP.

If your mail server requires authentication, check the box for "Enable use (SMTP) authentication" to log in to this server and enter the necessary information.

- **User Name/Password:** Enter the User Name and Password as provided by your network administrator or ISP (Internet Service Provider).

To ensure that the login procedure is performed as securely as possible when using SMTP authentication, you must define the weakest authentication method allowed.

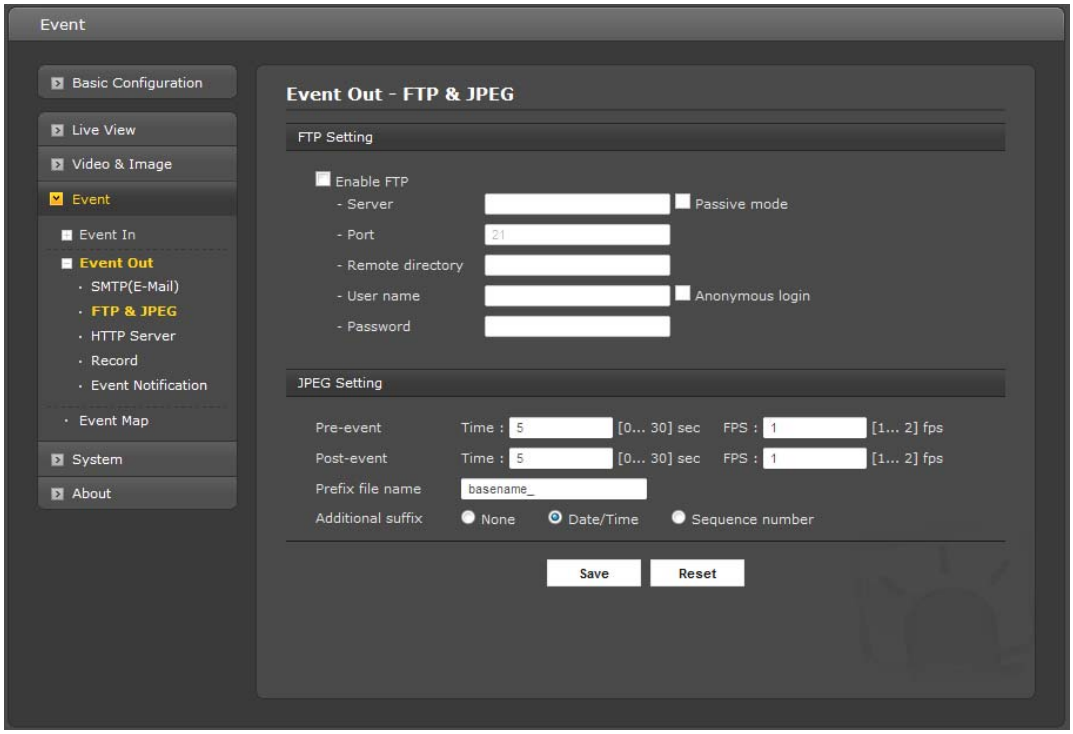
- **Login Method:** Set the weakest method allowed to the highest/safest method supported by the mail server. The most secure method is listed in the drop-down list:
  Login / Plain

- **SMTP (E-Mail) Receiver**
  - **Receiver:** Enter an email address for a receiver. You can register up to 8 e-mail addresses of recipients.

- **SMTP (E-Mail) Test**
  - **Receiver:** Enter an email address and click the Test button to test that the mail servers are functioning and that the email address is valid.

When the settings are complete, click **Save**, or click **Reset** to revert to previously saved settings.

▼ FTP & JPEG



When the network camera detects an event, it can record and save images to an FTP server. Images can be sent as e-mail attachments. Check the box to enable the service.

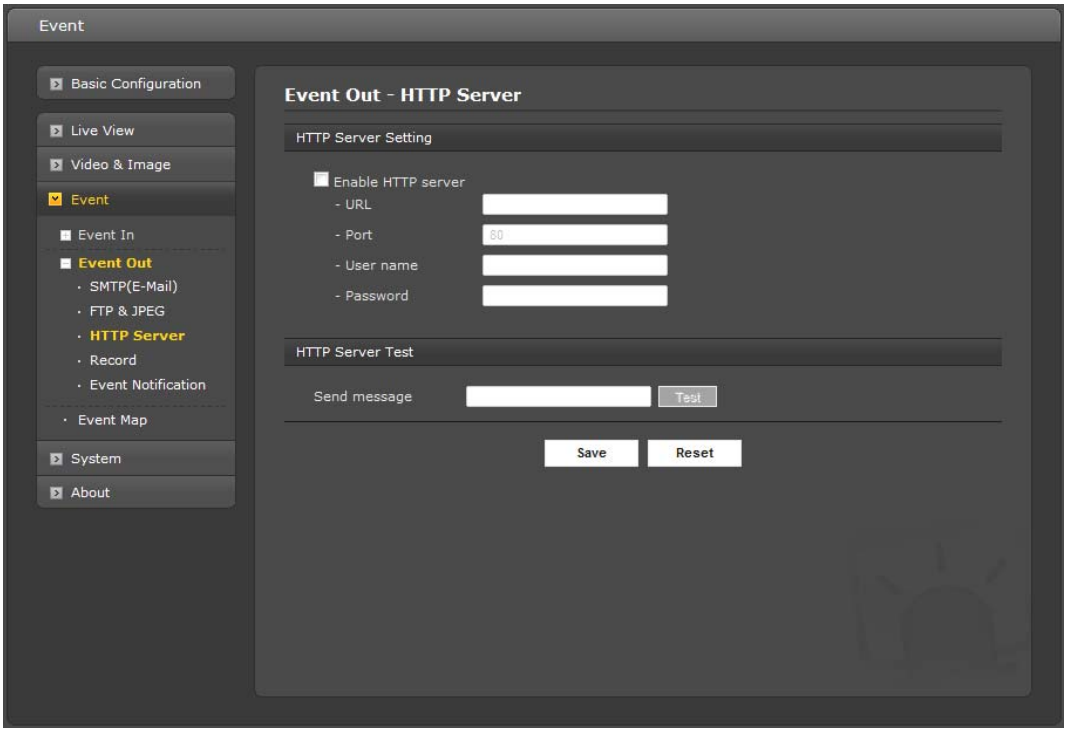
- **FTP Setting**
  - **Server:** Enter the server's IP address or host name. Note that a DNS server must be specified in the TCP/IP network settings if using a host name.
  - **Port:** Enter the port number used by the FTP server. The default is 21.
  - **Passive mode:** Under normal circumstances the network camera simply requests the target FTP server to open the data connection. Checking this box issues a PASV command to the FTP server and establishes a passive FTP connection, whereby the network camera actively initiates both the FTP control and data connections to the target server. This is normally desirable if there is a firewall between the camera and the target FTP server.

- **Remote directory:** Specify the path to the directory where the uploaded images will be stored. If this directory does not already exist on the FTP server, there will be an error message when uploading.
- **User name/Password:** Provide your log-in information.

- **JPEG Setting**
  - **Pre-event:** A pre-event buffer contains images from the time immediately preceding the event trigger. These are stored internally in the server. This buffer can be very useful when checking to see what happened to cause the event trigger. Enter the desired total length in seconds and specify the required frame-rate (fps).
  - **Post-event:** This function is the counterpart to the pre-trigger buffer described above and contains images from the time immediately after the trigger. Configure as for pre-event.
  - **Prefix file name:** This name will be used for all the image files saved. If suffixes are also used, the file name will take the form <prefix>.<suffix>.<extension>
  - **Additional suffix:** Add either a date/time suffix or, a sequence number - with or without a maximum value

When the settings are complete, click **Save**, or click **Reset** to revert to previously saved settings.

▼ HTTP Server

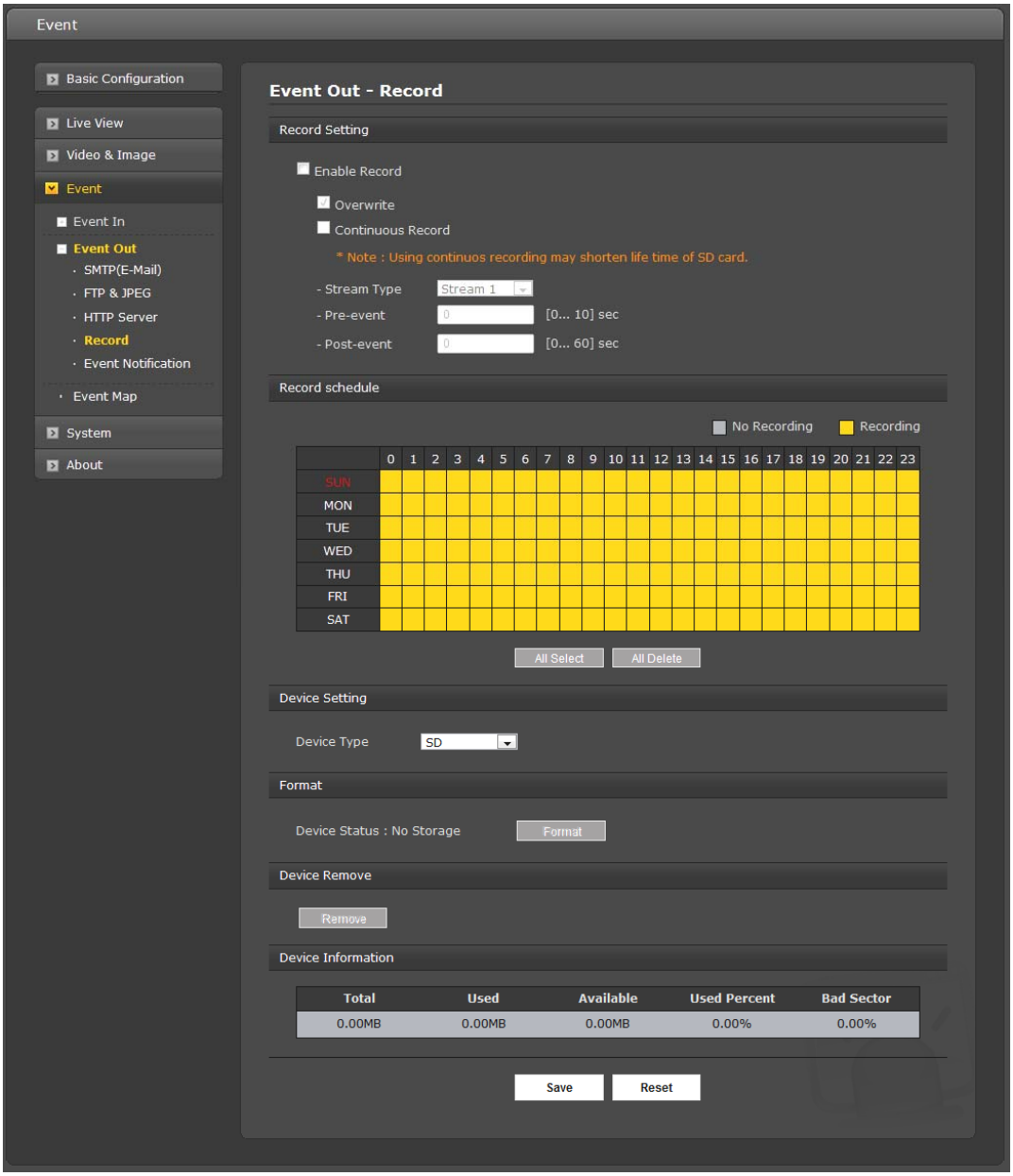


When the network camera detects an event, HTTP Server is used to receive uploaded image files and/or notification messages. Check the box to enable the service.

- **HTTP Server Setting**
  - **URL:** The network address to the server and the script that will handle the request. For example: http://192.168.12.244/cgi-bin/upload.cgi
  - **User name/Password:** Provide your log-in information.

- **HTTP Server Test**
  When the setup is complete, the connection can be tested by clicking the Test button.

▼ Record



When the network camera detects an event, it can record video stream in the Micro SD Memory (not supplied) or NAS (Network Attached Device) as a storage device. Check the box to enable the service.

- **Record Setting**
  - **Overwrite:** Click checkbox to overwrite the storage device.
  - **Stream Type:** You can select Stream1, Stream2, or Stream3.
    * **Stream1:** H.264 or MPEG-4 data.
    * **Stream2:** MJPEG data.
    * **Stream3:** H.264 or MPEG-4 data.
  - **Pre-event:** Enter pre-event time value for storage device pre-recording.
  - **Post-event:** Enter post-event time value for storage device post-recording.

- **Record Schedule**

The weekly recording schedule can be set for each day. Drag or click a box area; clicking the block toggles the recording between on and off. Click the “All Select” button to set a schedule for the entire week, 24/7; to record for a whole day, click in the “0” box and drag to “23”.

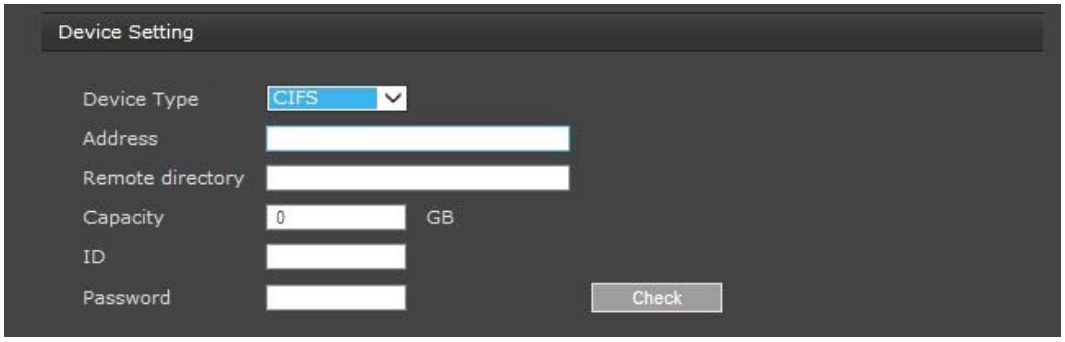
Note that the time is in 24 hour format, where 0 indicates midnight.

- **Device Setting**

  Select Device Type to be recorded in the drop-down list. The screen changes according to selection.
  - **SD:** Built-in SD card
  - **CIFS:** A file format for a NAS device.
  - **NFS:** A file format for a NAS device.

Note 1: Common Internet File System (CIFS) is a remote file access protocol that forms the basis for Windows file sharing, network printing, and various other network services. CIFS requires a large number of request/response transactions and its performance degrades significantly over high-latency WAN links such as the Internet.
Note 2: Network File System (NFS) is a network file system protocol, allowing a user on a client computer to access files over a network in a manner similar to how local storage is accessed. NFS, like many other protocols, builds on the Open Network Computing Remote Procedure Call (ONC RPC) system.

The CIFS screen displays as below.



* **Address:** Enter IP address for NAS device.
* **Remote Directory:** Enter directory or folder location to be recorded in the NAS device.
* **Capacity:** Enter the capacity of storage to be used. It must be less than the total storage capacity.
* **IP/Password:** Enter ID and Password. The network camera will ask them whenever you access NAS device.
* **Check:** Press the Check button to check the validity of Device Setting data.

- **Format**

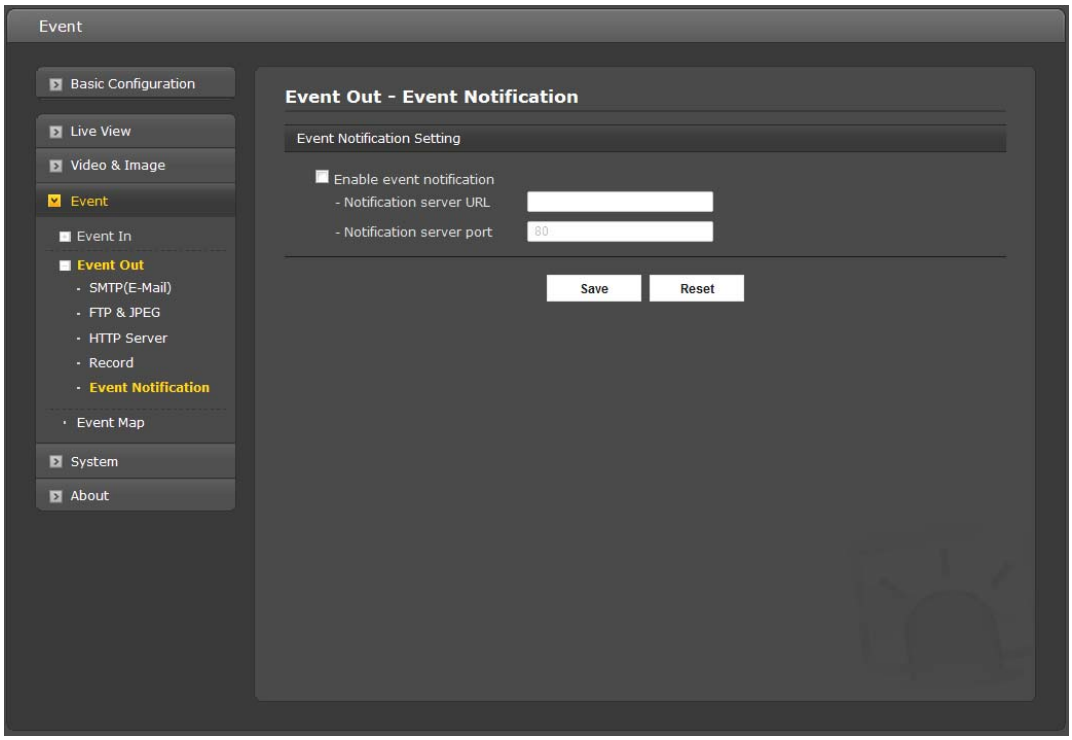
  Click the Format button to format SD card.

- **Device Information**

  Show current SD card information.

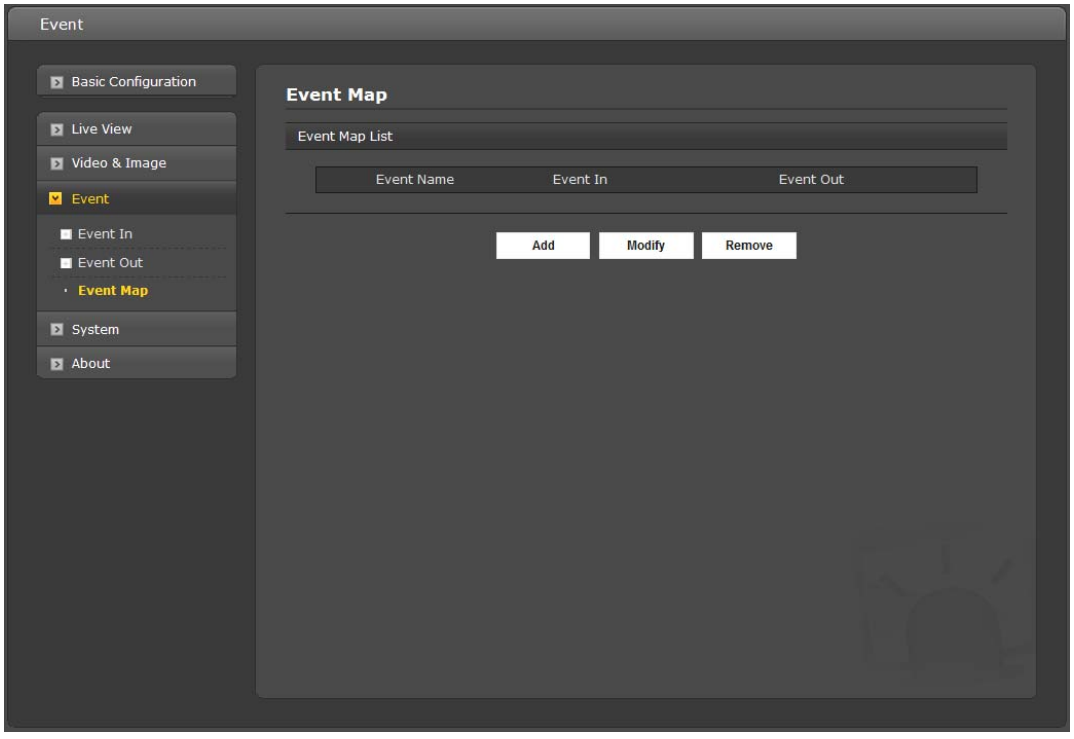
When the settings are complete, click **Save**, or click **Reset** to revert to previously saved settings.

▼ Event Notification



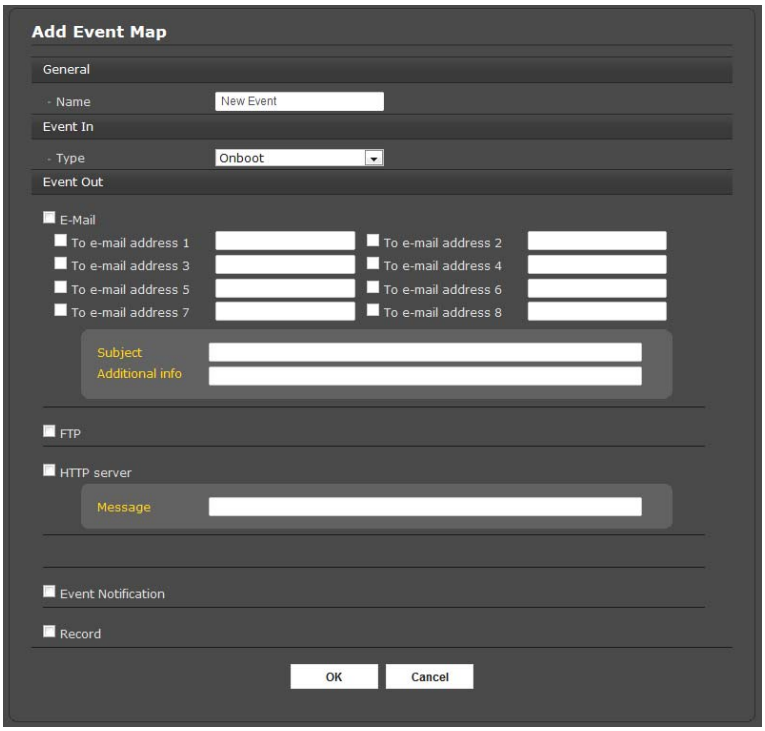
When the network camera detects an event, it can send a message to a designated server that this event has occurred. Check the "Enable event notification" box to enable the service. Enter the notification server URL and port.

3) Event Map



The event map allows you to change the settings and establish a schedule for each event trigger from the network camera. You can register the event map up to max. 15.

Click the Add button to make a new event map; a popup window displays as below. To change an existing event, select that event and click the Modify button; this same window will display and the information can be changed as required. Selecting an event and clicking Remove deletes the event.



- **General**
  Enter the name for a new event map.

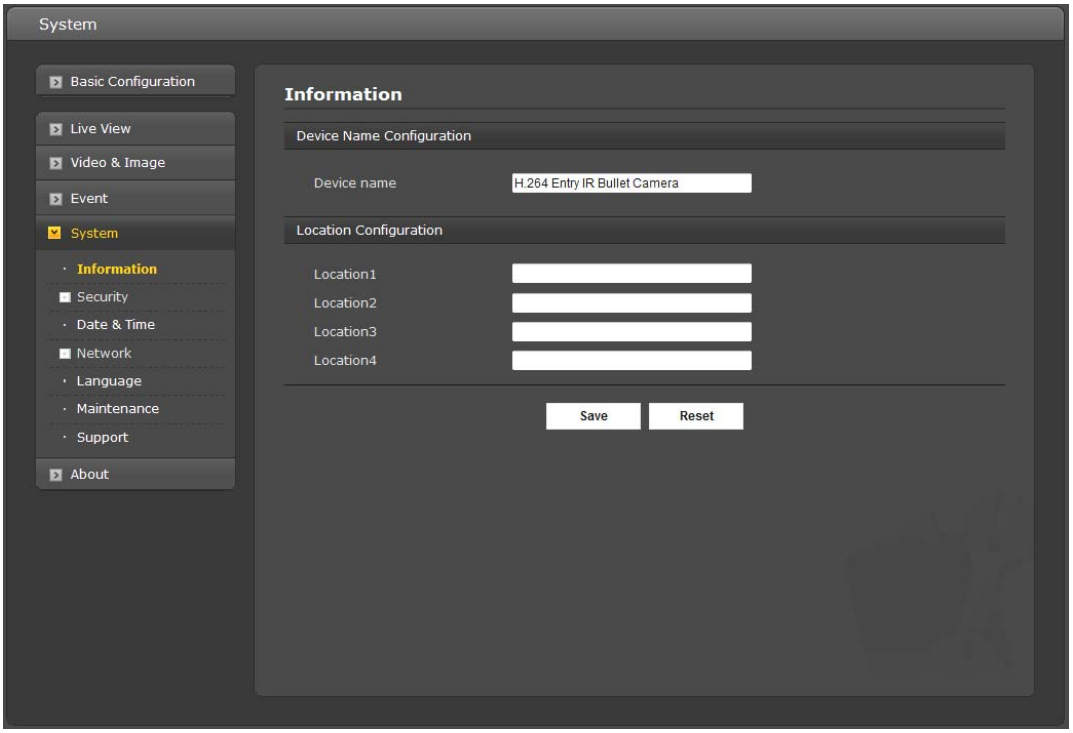
- **Event In**
  Select an event type in the drop down list.

- **Event Out**
  - **E-mail:** Select email addresses you want to send via email that an event has occurred.
  - **FTP:** Select checkbox beside FTP to record and saves images to an FTP server when an event has occurred.
  - **HTTP Server:** Send notification messages to a HTTP server that listens for these. The destination server must first be configured on the Event In page. Enter a message you want to send.
  - **Event Notification:** Sends XML messages to an Notification server that listens for these. The destination server must first be configured on the Event In page.
  - **Record:** Record video stream when an event has occurred. The Record option must first be configured on the Event Out page. When the network camera detects an event, it can record video stream in the Micro SD Memory (not supplied) or NAS (Network Attached Device) as a storage device. Check the Record box to enable the function.

3.5.5 System

1) Information

You can enter the system information. This page is very useful as a reference for information after installation.



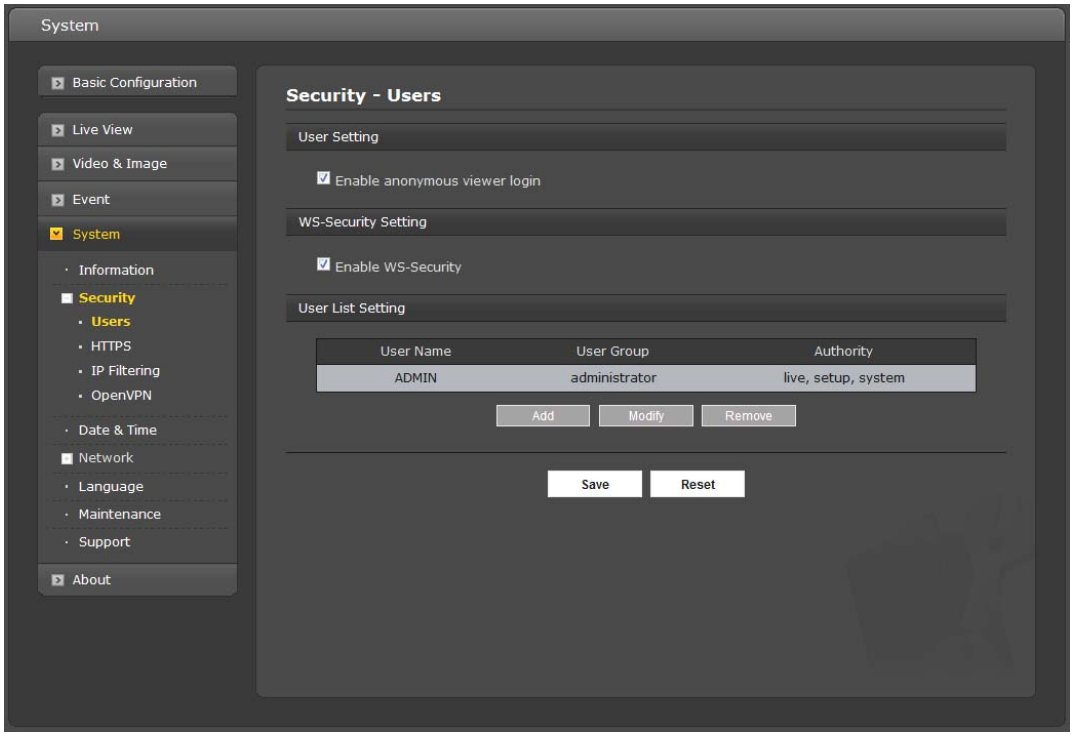
- **Device Name Configuration**
  Enter the device name.

- **Location Configuration**
  Enter the location information. You can enter up to four locations.

When the settings are complete, click **Save**, or click **Reset** to revert to previously saved settings.

2) Security

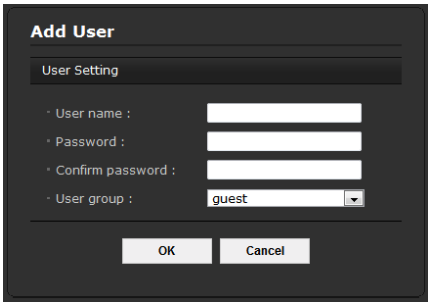
▼ Users



User access control is enabled by default, when the administrator sets the root password on first access. New users are authorized with user names and passwords, or the administrator can choose to allow anonymous viewer login to the Live View page, as described below:

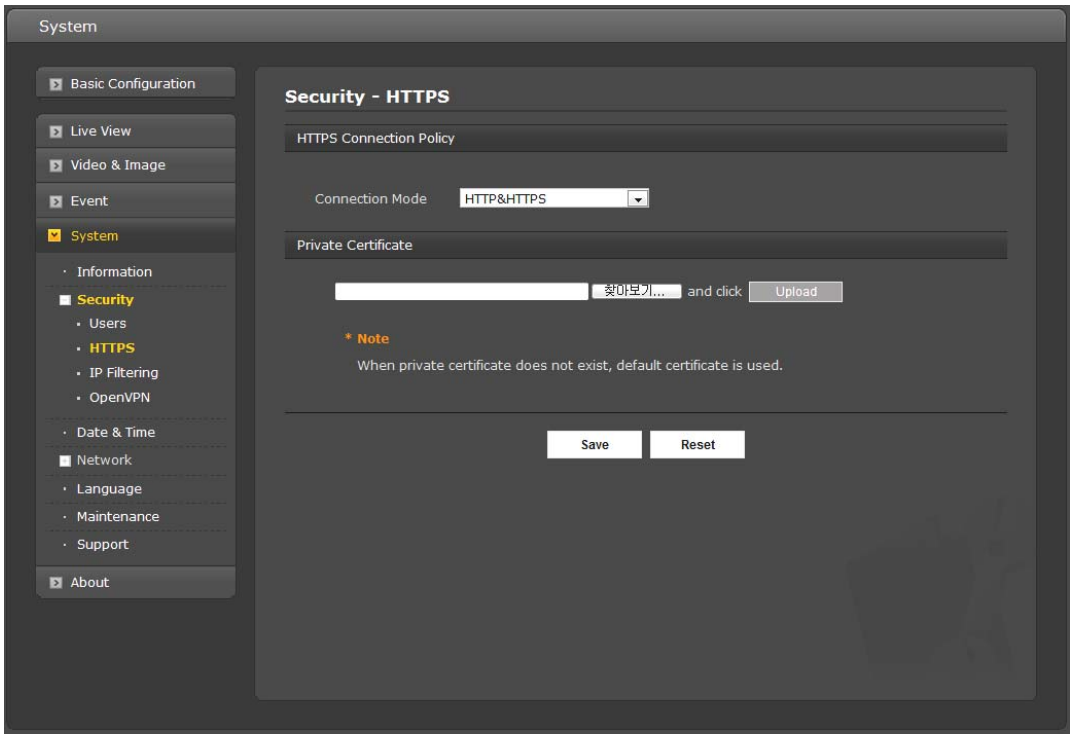
- **User Setting**
  Check the box to "Enable anonymous viewer login" to the network camera without a user account. When using the user account, users have to log-in at every access.

- **User List Setting**
  This section shows a list of registered user accounts. Press the Add button; the pop-up window displays as below. Enter a user name and password to be added and select the user group from the drop-down list; click OK to register the user or Cancel to negate the user. User information can also be modified by selecting the user from the list and clicking the Modify button; this same screen will display. Change any information as needed. Selecting a user and clicking Remove deletes the user.



When the settings are complete, click **Save**, or click **Reset** to revert to previously saved settings.

▼ HTTPS



For greater security, the network camera can be configured to use HTTPS [Hypertext Transfer Protocol over SSL (Secure Socket Layer)], so that all communication that would otherwise go via HTTP will instead go via an encrypted HTTPS connection.

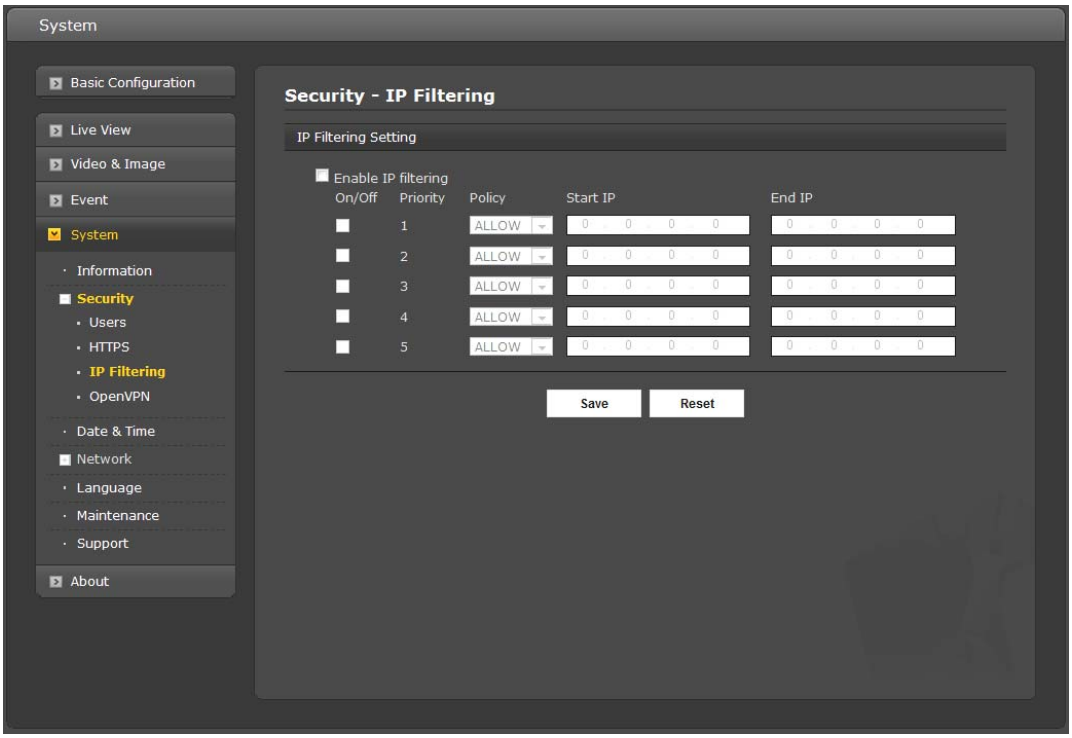
- **HTTPS Connection Policy**
  Choose the form of connection you wish to use from the drop-down list for the Administrator, Operator and Viewer to enable HTTPS connection (set to HTTP by default).
  - **HTTP**
  - **HTTPS**
  - **HTTP & HTTPS**

- **Private Certificate**
  To use HTTPS for communication with the network camera, an official certificate issued by a CA (Certificate Authority) must be uploaded from your PC. Provide the path to the certificate directly, or use the **Browse** button to locate it. Then click the **Upload** button.

Refer to the home page of your preferred CA for information on where to send the request.

When the settings are complete, click **Save**, or click **Reset** to revert to previously saved settings.

▼ IP Filtering



Checking the "Enable IP address filtering" box enables the IP address filtering function. When the IP address filter is enabled, addresses added to the list are set as allowed or denied addresses. All other IP addresses not in this list will then be allowed or denied access accordingly, that is, if the addresses in the list are allowed, then all others are denied access, and vice versa.

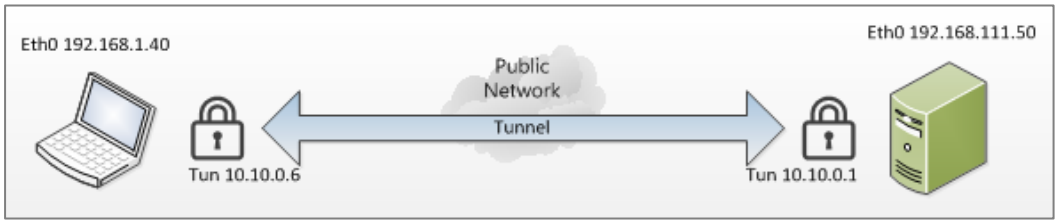
Note that users from IP addresses that will be allowed must also be registered with the appropriate access rights (Guest, Operator or Administrator). This is done from Setup> System>Security>Users.

When the settings are complete, click **Save**, or click **Reset** to revert to previously saved settings.

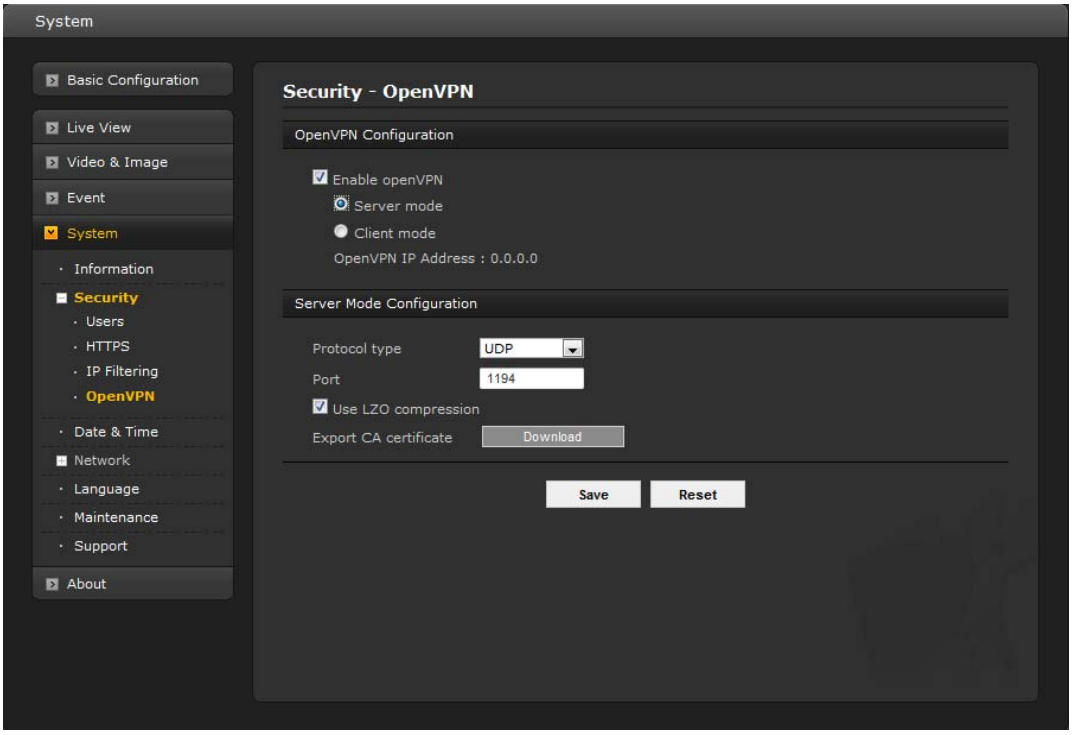
▼ OpenVPN

OpenVPN is an open source software application that implements virtual private network (VPN) techniques for creating secure point-to-point or site-to-site connections in routed or bridged configurations and remote access facilities.

- OpenVPN can run over User Datagram Protocol (UDP) or Transmission Control Protocol (TCP) transports; multiplexing creates SSL tunnels on a single TCP/UDP port.
- OpenVPN uses the OpenSSL library to provide encryption of both the data and control channels.
- OpenVPN offers two types of interfaces for networking via the Universal TUN/TAP driver. It can create either a layer-3 based IP tunnel (TUN), or a layer-2 based Ethernet TAP that can carry any type of Ethernet traffic.



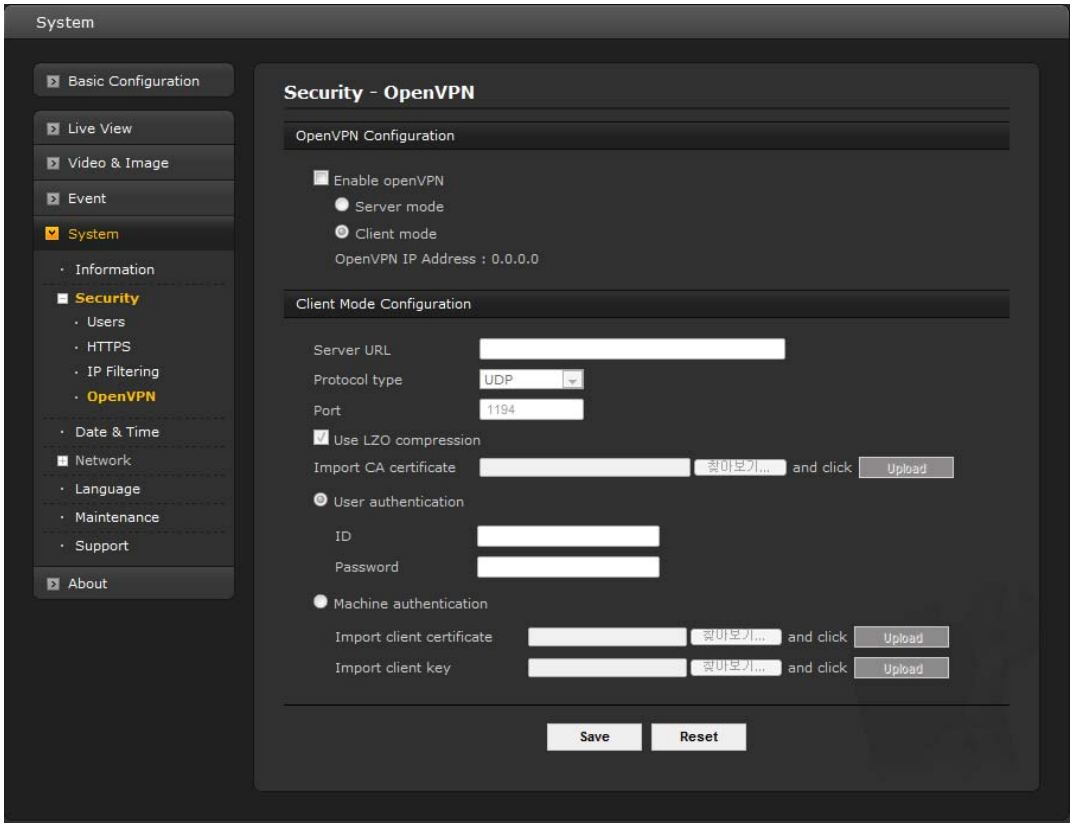
Note: It has the ability to work through most proxy servers (including HTTP) and is good at working through Network address translation (NAT) and getting out through firewalls.



- **OpenVPN Configuration**
  Check the box to enable OpenVPN and select mode.
  - **Server Mode:** Network camera operates as an OpenVPN Server.
  - **Client Mode:** Network camera operates as an OpenVPN Client.

- **Server Mode Configuration**
  - **Protocol type:** Choose Protocol type, either UDP or TCP; UDP is preferred.
  - **Port:** Type in Port number you want to use; default is 1194.
  - **Use LZO compression:** Determines whether to use cypher compression in connection.
  - **Export CA certificate:** Download the CA certificate issued by Server for Client setup.

  After finishing setup, click Save button; the camera now operates as an OpenVPN Server.

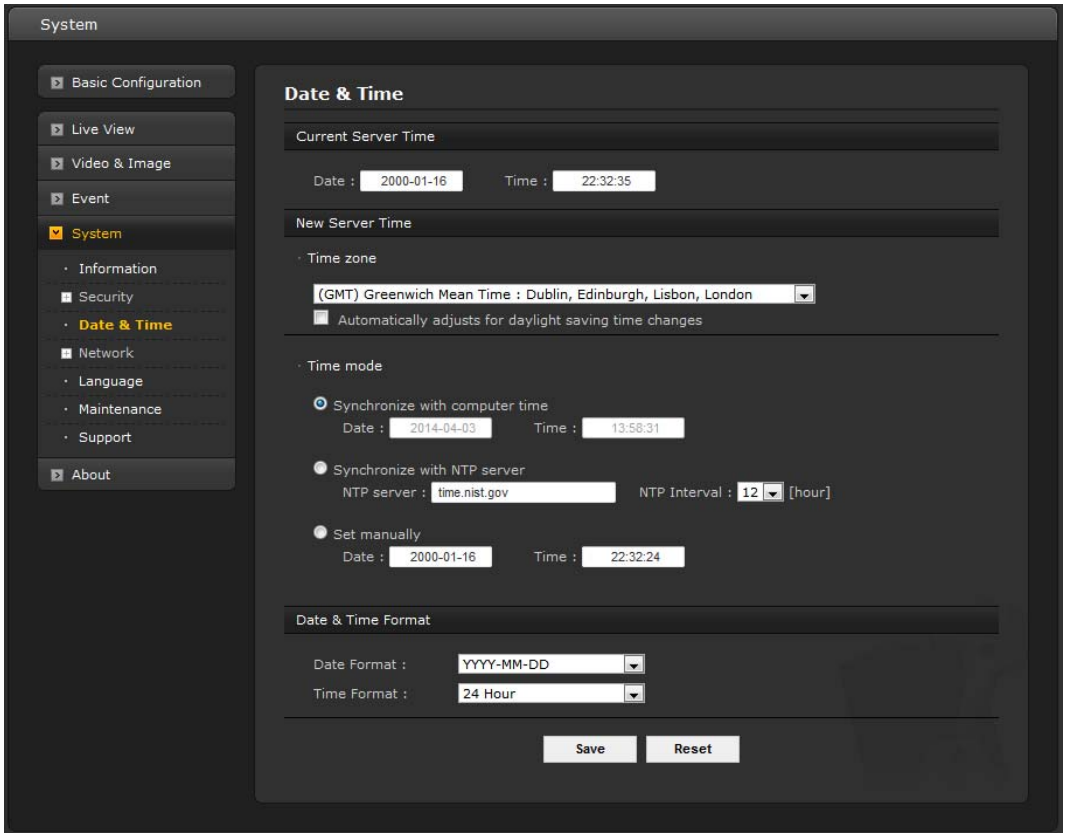


- **Client Mode Configuration**
  - **Server URL:** Shows OpenVPN Server URL after the connection is established.
  - **Protocol type:** Enter the same as Server setting.
  - **Port:** Enter the same as Server setting.
  - **Use LZO compression:** Must be same as Server setting.
  - **Import CA certificate:** Upload the CA certificate issued by Server for Client setup.

  Select authentication method, either User authentication or Machine authentication.
  - **User authentication:** Enter registered ID and Password.
  - **Machine authentication:** Upload client certificate and client key provided by Server.

  After finishing setup, click Save button; the camera now operates as an OpenVPN Client.

3) Date & Time



- **Current Server Time**
  It displays the current date and time (24h clock). The time can be displayed in 12h clock format (see below).

- **New Server Time**
  Select your time zone from the drop-down list. If you want the server clock to automatically adjust for daylight savings time, select “Automatically adjusts for daylight saving time changes”.

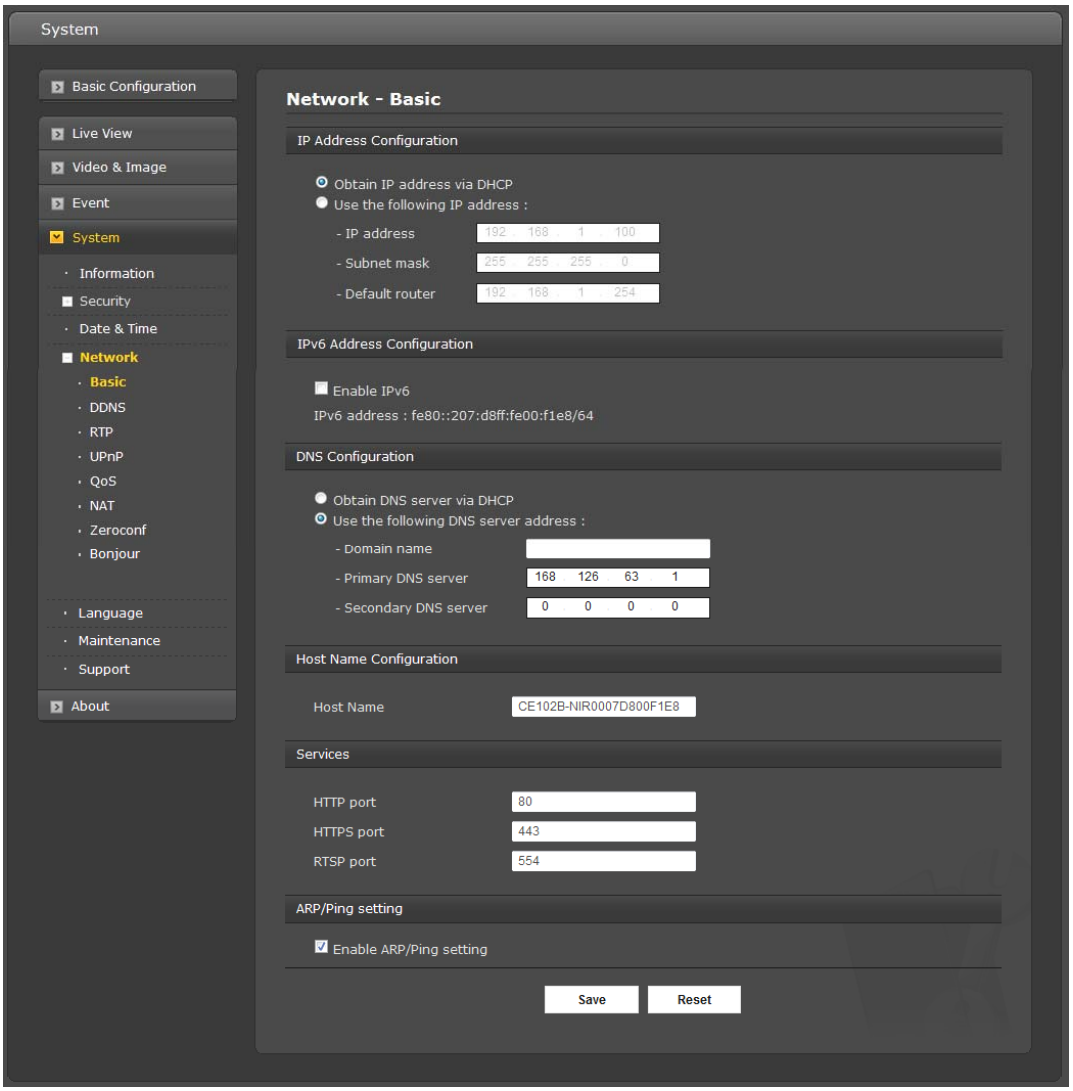
  From the **Time Mode** section, select the preferred method to use for setting the time:
  - **Synchronize with computer time:** Sets the time from the clock on your computer.
  - **Synchronize with NTP Server:** The network camera will obtain the time from an NTP server every 60 minutes.
  - **Set manually:** Allows you to manually set the time and date.

- **Date & Time Format**
  Specify the formats for the date and time (12h or 24h) displayed in the video streams.
  Select Date & Time format from the drop-down list.
  - **Date Format:** Specify the date format. YYYY: Year, MM: Month, DD: Day
  - **Time Format:** Specify the date format. 24 Hours or 12 Hours

When the settings are complete, click **Save**, or click **Reset** to revert to previously saved settings.

Note: Note that if using a host name for the NTP server, a DNS server must be configured under TCP/IP settings.

4) Network



Setting in regard to network can be executed. Settings for IP, DNS, Host Name, Port, and ARP/Ping can be established, along with setting for DDNS, uPnP, QoS, Zeroconfig, Bonjour and wireless.

▼ Basic

- **IP Address Configuration:**
  - **Obtain IP address via DHCP:** Dynamic Host Configuration Protocol (DHCP) is a protocol that lets network administrators centrally manage and automate the assignment of IP addresses on a network. DHCP is enabled by default. Although a DHCP server is mostly used to set an IP address dynamically, it is also possible to use it to set a static, known IP address for a particular MAC address. To obtain IP address via DHCP, check the radio button.
  - **Use the following IP address:** To use a static IP address for the network camera, check the radio button and then make the following settings:
  * **IP address:** Specify a unique IP address for your network camera.
  * **Subnet mask:** Specify the mask for the subnet the network camera is located on.

* **Default router:** Specify the IP address of the default router (gateway) used for connecting devices attached to different networks and network segments.

- **IPv6 Address Configuration**
  Check this box to enable IPv6. Other settings for IPv6 are configured in the network router.

- **DNS Configuration**
  DNS (Domain Name Service) provides the translation of host names to IP addresses on your network. Check the radio button to obtain DNS server via DHCP or set the DNS server.
  - **Obtain DNS Server via DHCP:** Automatically use the DNS server settings provided by the DHCP server.
  - Use the following DNS server address to enter the desired DNS server by specifying the following:
  * **Domain name:** Enter the domain(s) to search for the host name used by the network camera. Multiple domains can be separated by semicolons (;). The host name is always the first part of a Fully Qualified Domain Name, for example, myserver is the host name in the Fully Qualified Domain Name myserver.mycompany.com where mycompany.com is the Domain name.
  * **DNS servers:** Enter the IP addresses of the primary and secondary DNS servers.

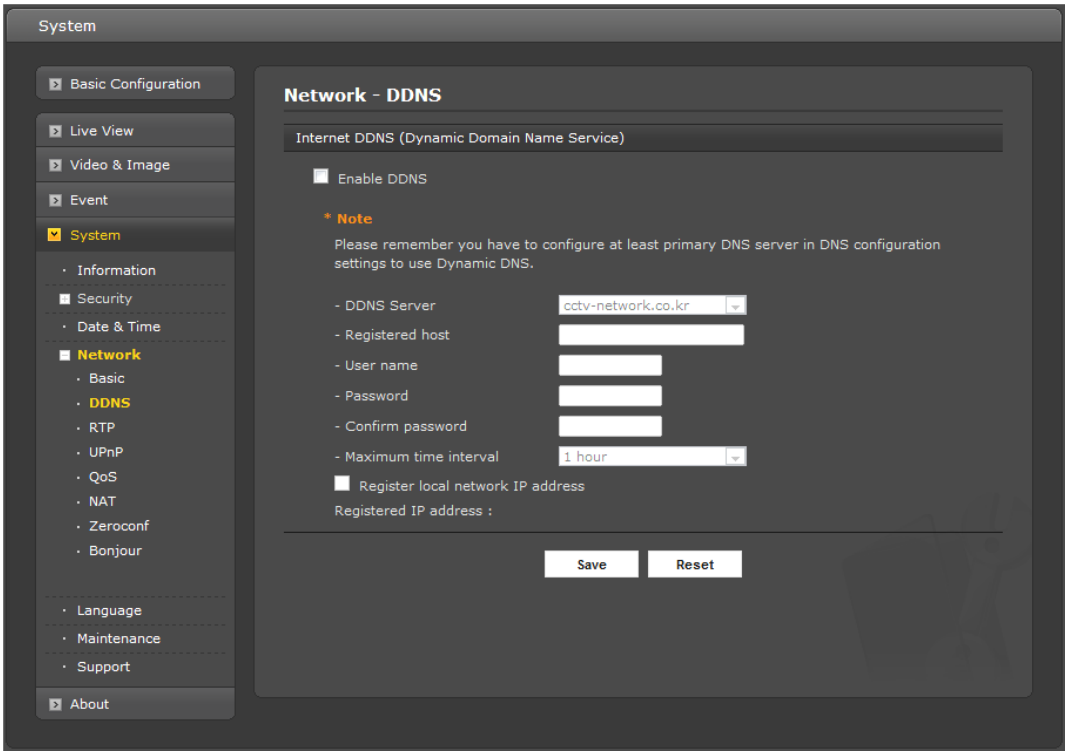
- **Host Name Configuration**
  - **Host Name** – Enter the host name to be used as device information in the client software or SmartManager. This is the camera name that will show up in the Site List in ViconNet.

- **Services**
  - **HTTP port:** Enter a port to receive a service through the HTTP. Default port number is '80'.
  - **HTTPS port:** Enter a port to receive a service through the HTTPS. Default port number is '443'.
  - **RTSP port:** Enter a port to receive a service through the RTSP. Default port number is '554'.

- **ARP/Ping Setting**
  - **Enable ARP/Ping setting:** The IP address can be set using the ARP/Ping method, which associates the unit's MAC address with an IP address. Check this box to enable the service.
    Leave disabled to prevent unintentional resetting of the IP address.

When the settings are complete, click **Save**, or click **Reset** to revert to previously saved settings.

▼ DDNS

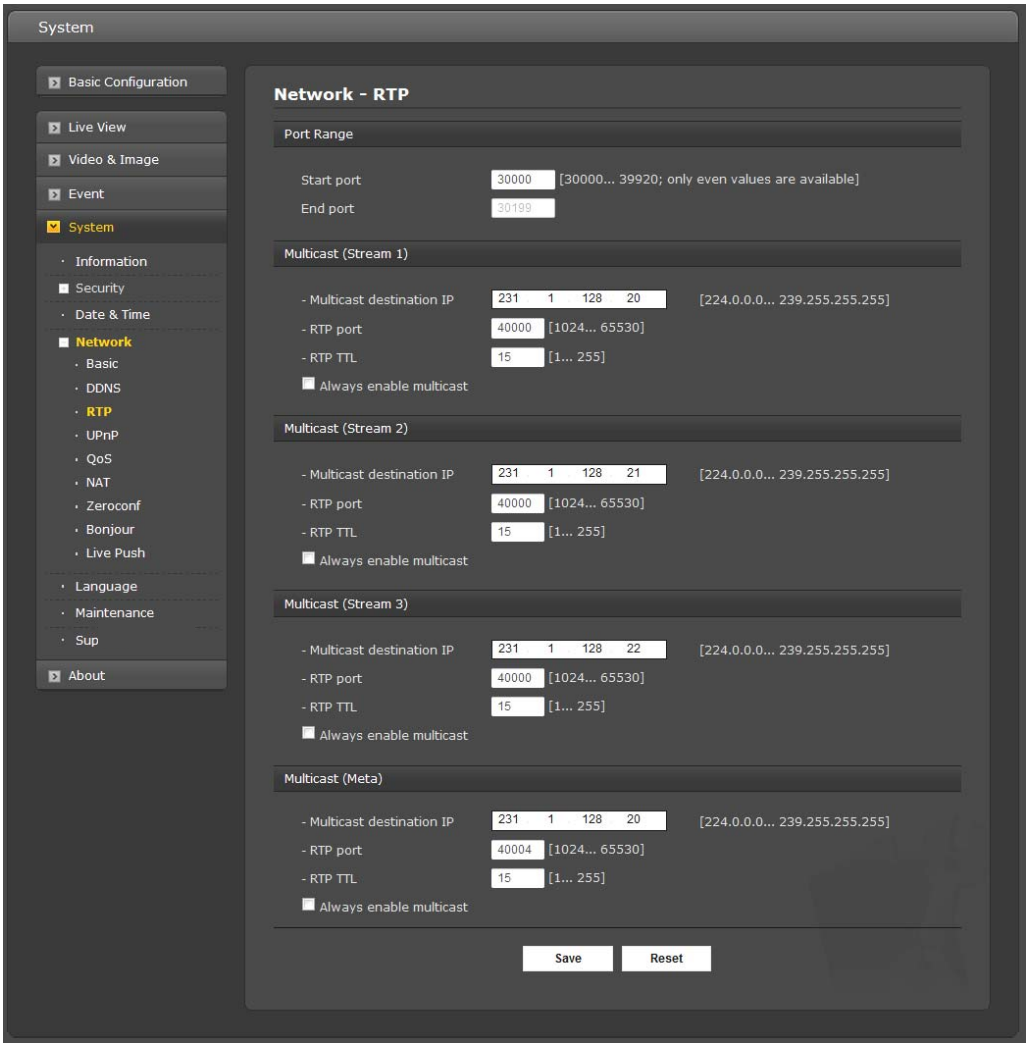


- **Internet DDNS (Dynamic Domain Name Service)**
  When using the high-speed Internet with the telephone or cable network, users can operate the Network Camera even on the floating IP environment in which IPs are changed at every access. Users should receive an account and password by visiting a DDNS service like http://www.dyndns.com/,

  - **Enable DDNS:** Check to get DDNS service to be available.
  * **DDNS Server:** Select the DDNS server.
  * **Registered host:** Enter an address of the DDNS server.
  * **Username:** Enter an ID to access to the DDNS server.
  * **Password:** Enter a password to be used for accessing the DDNS server.
  * **Confirm:** Enter the password again to confirm it.
  * **Maximum time interval:** Set a time interval to synchronize with the DDNS server. Select the time interval from the drop-down list.
  * **Register local network IP address:** Register a Network Video Server IP address to the DDNS server by checking the box and enter the Registered IP address.

When the settings are complete, click **Save**, or click **Reset** to revert to previously saved settings.

▼ **RTP**



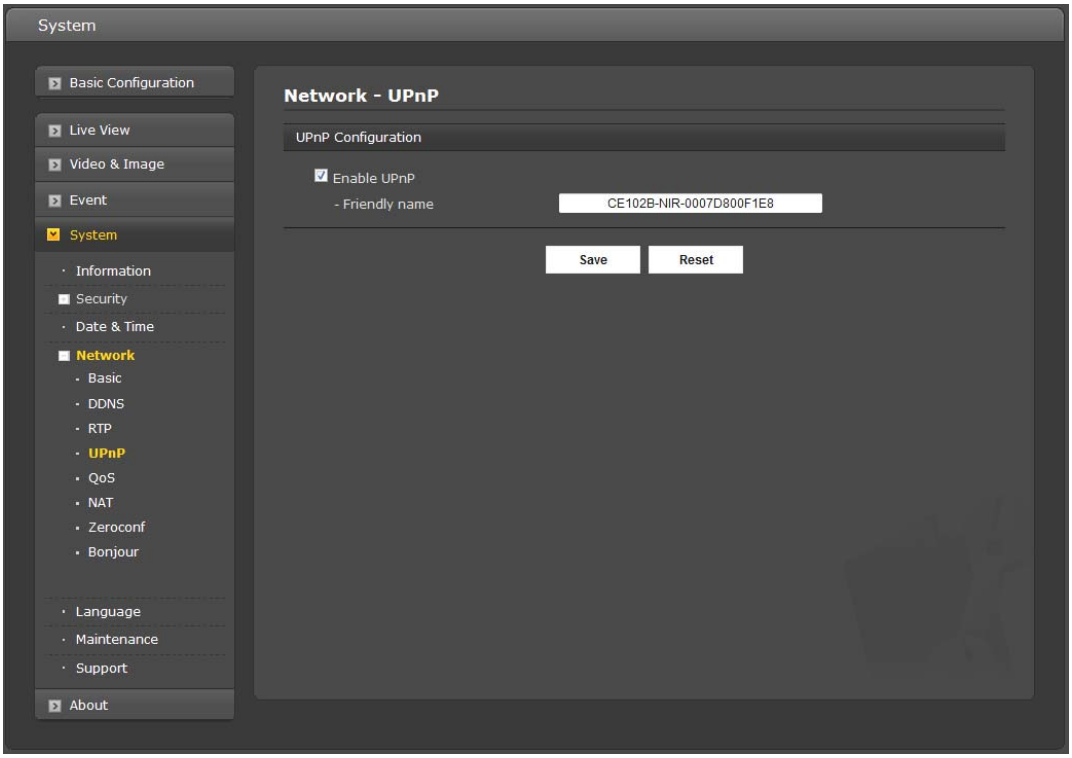
Create a setting for sending and receiving video on a real-time basis. These settings are the IP address, port number, and Time-To-Live value (TTL) to use for the media stream(s) in multicast H.264 format. Only certain IP addresses and port numbers should be used for multicast streams.

- **Port Range**
  - **Start / End port:** Enter a value between 30000 and 39920

- **Multicast**
  This function is for sending Video to Multicast group.
  - **Enable Multicast:** Check the checkbox to enable multicast operation.
  - **Multicast destination IP:** Enter an IP between 224.0.0.0 and 239.255.255.255.
  - **RTP port:** Enter a value between 1024 and 65530.
  - **RTP TTL:** Enter a value between 1 and 255. If a network status is smooth, enter a lower value. However, if a network status is poor, enter a higher value. When there are many network cameras or users, a higher value may cause a heavy load to the network. Consult with a network manager for detailed information.
  - **Always enable multicast:** Check the box to start multicast streaming without opening an RTSP session.

When the settings are complete, click **Save**, or click **Reset** to revert to previously saved settings.

▼ UPnP



The network camera includes support for UPnP™. UPnP is enabled by default, so the network camera is automatically detected by operating systems and clients that support this protocol. Enter a name in the Friendly name field.

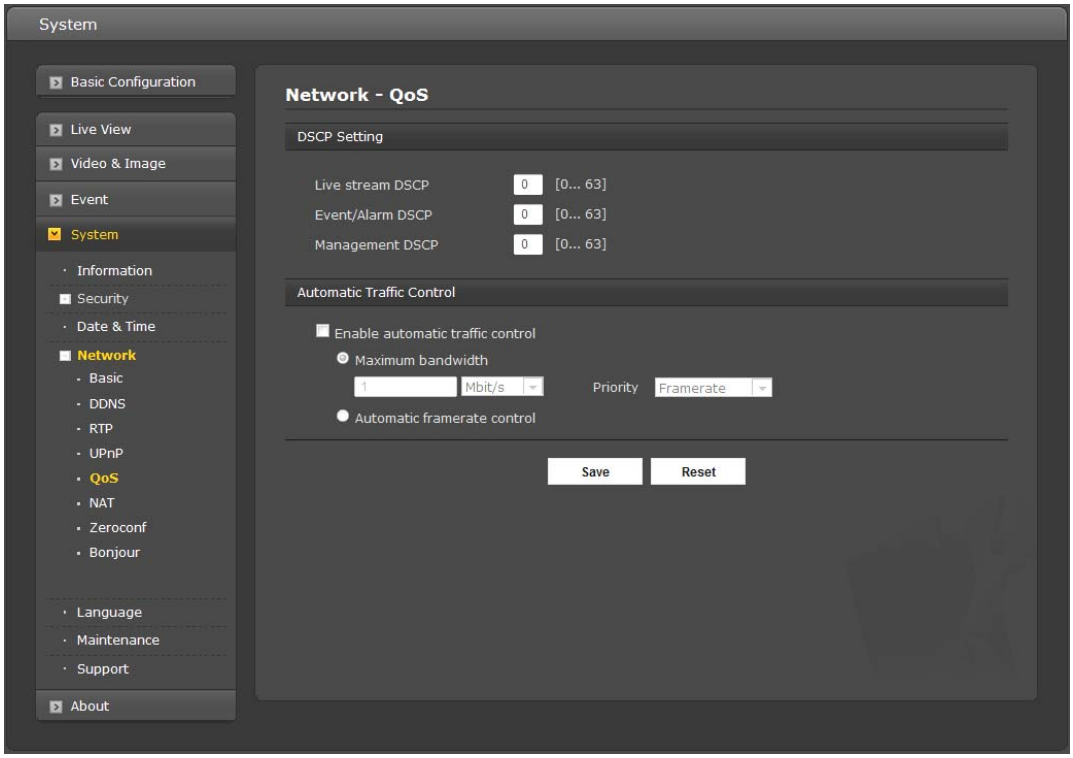
Note: UPnP must be installed on your workstation if running Windows XP. To do this, open the Control Panel from the Start Menu and select Add/Remove Programs. Select Add/Remove Windows Components and open the Networking Services section. Click Details and then select UPnP as the service to add.

▼ QoS

Quality of Service (QoS) provides the means to guarantee a certain level of a specified resource to selected traffic on a network. Quality can be defined as a maintained level of bandwidth, low latency, and no packet losses.

The main benefits of a QoS-aware network are:

- The ability to prioritize traffic and thus allow critical flows to be served before flows with lesser priority.
- Greater reliability in the network, due to the control of the amount of bandwidth an application may use, and thus control over bandwidth races between applications.



- **DSCP Settings**
  For each type of network traffic supported by your network video product, enter a DSCP (Differentiated Services Code Point) value. This value is used to mark the traffic's IP header. When the marked traffic reaches a network router or switch, the DSCP value in the IP header tells the router or switch which type of treatment to apply to this type of traffic, for example, how much bandwidth to reserve for it. Note that DSCP values can be entered in decimal or hex form, but saved values are always shown in decimal.

  The following types of traffic are marked:
  - **Live Stream DSCP:**
  - **Event/Alarm DSCP:**
  - **Management DSCP:**

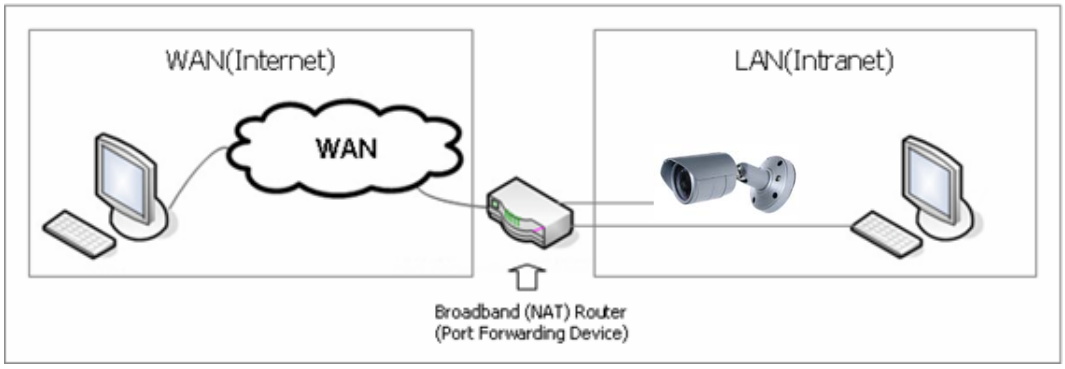
- **Automatic Traffic Control**
  Check the box to enable automatic traffic control.
  Set a limitation on user network resources by designating the maximum bandwidth. Select either the Maximum bandwidth or Automatic frame rate radio button.
  - **Maximum bandwidth:** When sharing other network programs or equipment, it is possible to set a limitation on the maximum bandwidth in the unit of Mbit/s or kbit/s.
  - **Auto frame rate:** Selected if not influenced by a network-related program or equipment without a limitation on the network bandwidth.

When the settings are complete, click **Save**, or click **Reset** to revert to previously saved settings.

▼ NAT Traversal

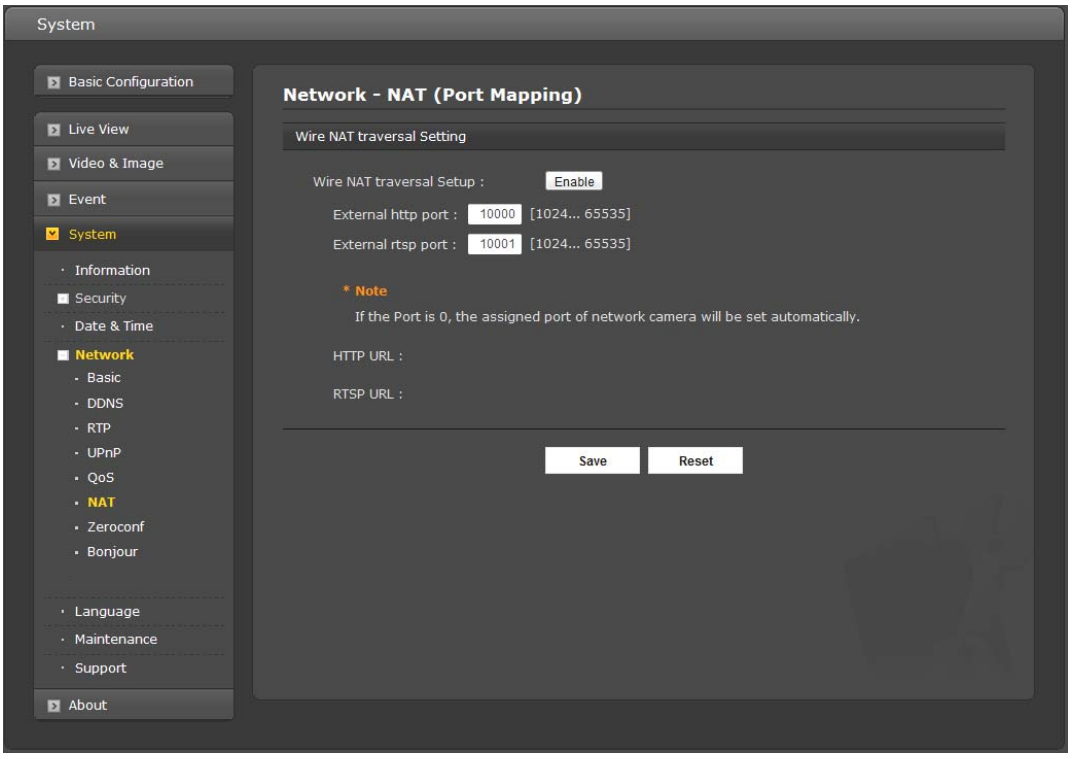
A broadband router allows devices on a private network (LAN) to share a single connection to the Internet. This is done by forwarding network traffic from the private network to the “outside”, that is, the Internet. Security on the private network (LAN) is increased since most broadband routers are pre-configured to stop attempts to access the private network (LAN) from the public network/Internet.

Use **NAT traversal** when your network cameras are located on an intranet (LAN) and you wish to make it available from the other (WAN) side of a NAT router. With NAT traversal properly configured, all HTTP traffic to an external HTTP port in the NAT router is forwarded to the network camera.



Notes:

- For NAT traversal to work, this must be supported by the broadband router.
- The broadband router has many different names:
  “NAT router”, “Network router“, Internet Gateway”, “Broadband sharing device” or “Home firewall” but the essential purpose of the device is the same.



- **NAT traversal Settings**
  - **Enable:** Click this button to enable NAT traversal. When enabled, the network camera attempts to configure port mapping in a NAT router on your network, using UPnP. Note that UPnP must be enabled in the network camera (see System>Network>UPnP).

    Enter a NAT router and enter the external port number for the router in the field provided. If you enter o in those fields, the network camera automatically searches for NAT routers on your network.

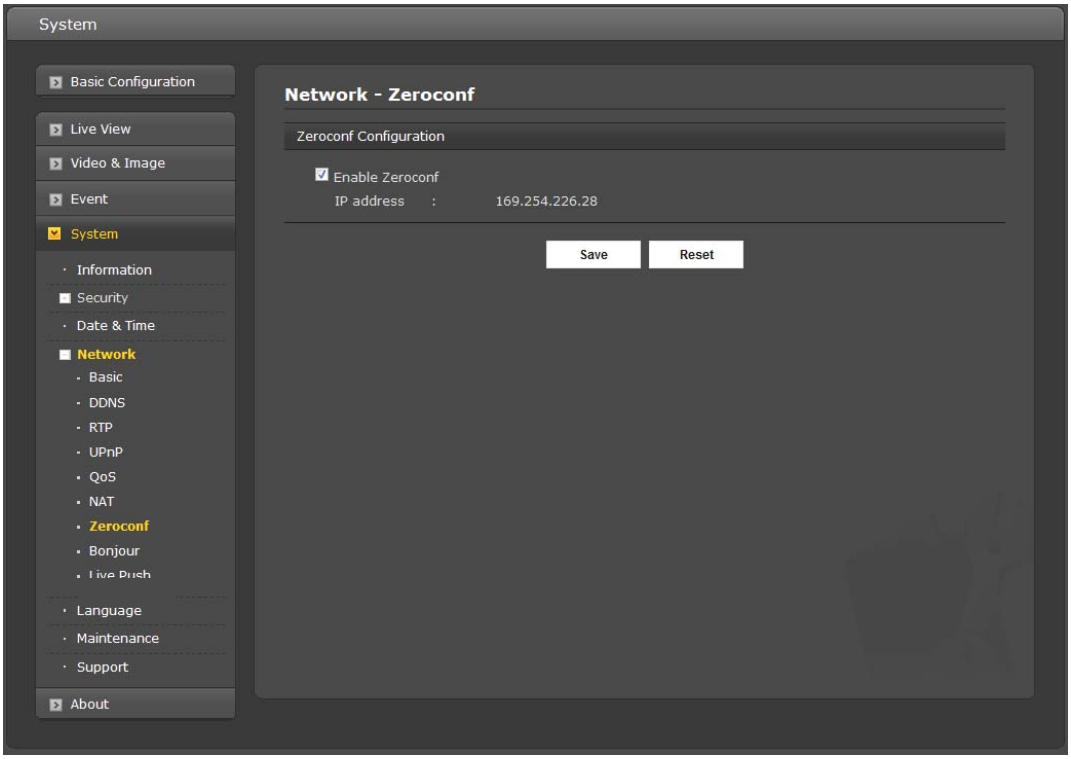
Notes:

- If you attempt to manually enter a port that is already in use, an alert message will be displayed.
- When the port is selected automatically it is displayed in this field. To change this enter a new port number and click Save.

When the settings are complete, click **Save**, or click **Reset** to revert to previously saved settings.

▼ Zeroconfig

Zeroconfig allows the network camera to create and assign IP address for network cameras and connect to a network automatically.



Zero configuration networking (zeroconf), is a set of techniques that automatically creates a usable Internet Protocol (IP) network without manual operator intervention or special configuration servers.

Zero configuration networking allows devices such as computers and printers to connect to a network automatically. Without zeroconf, a network administrator must set up services, such as Dynamic Host

Configuration Protocol (DHCP) and Domain Name System (DNS), or configure each computer's network settings manually, which may be difficult and time-consuming.

Zeroconf is built on three core technologies:

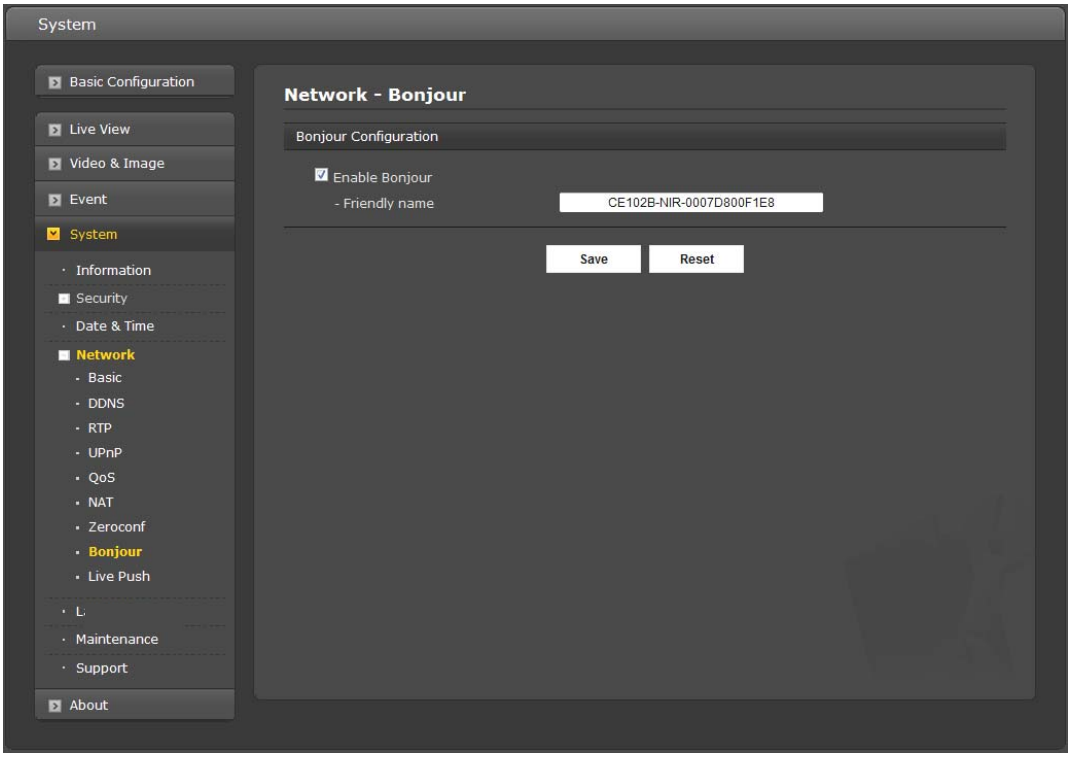
- Assignment of numeric network addresses for networked devices (link-local address auto configuration).
- Automatic resolution and distribution of computer hostnames (multicast DNS).
- Automatic location of network services, such as printing devices through DNS service discovery.

Click the check box to enable Zeroconf.

When the settings are complete, click **Save**, or click **Reset** to revert to previously saved settings.

▼ Bonjour

The network camera includes support for Bonjour. When enabled, the network camera is automatically detected by operating systems and clients that support this protocol.



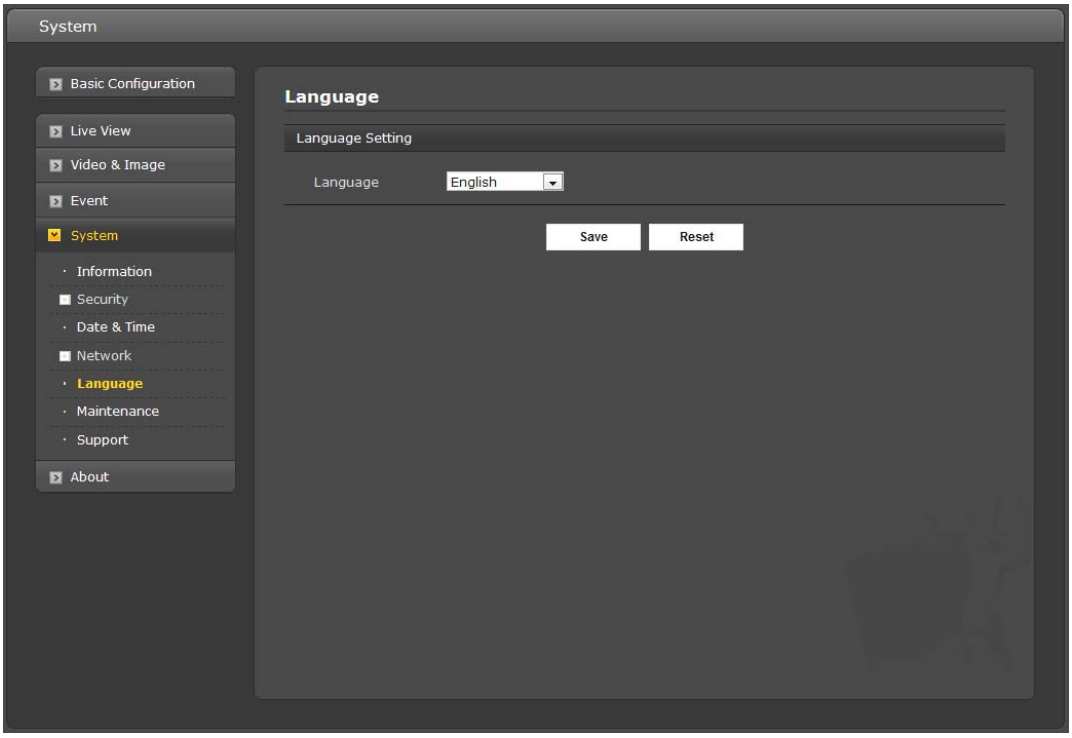
Click the check box to enable Bonjour. Enter a name in the Friendly name field.

When the settings are complete, click **Save**, or click **Reset** to revert to previously saved settings.

Note: Also known as zero-configuration networking, Bonjour enables devices to automatically discover each other on a network, without having to enter IP addresses or configure DNS servers. (Bonjour is a trademark of Apple Computer, Inc.)

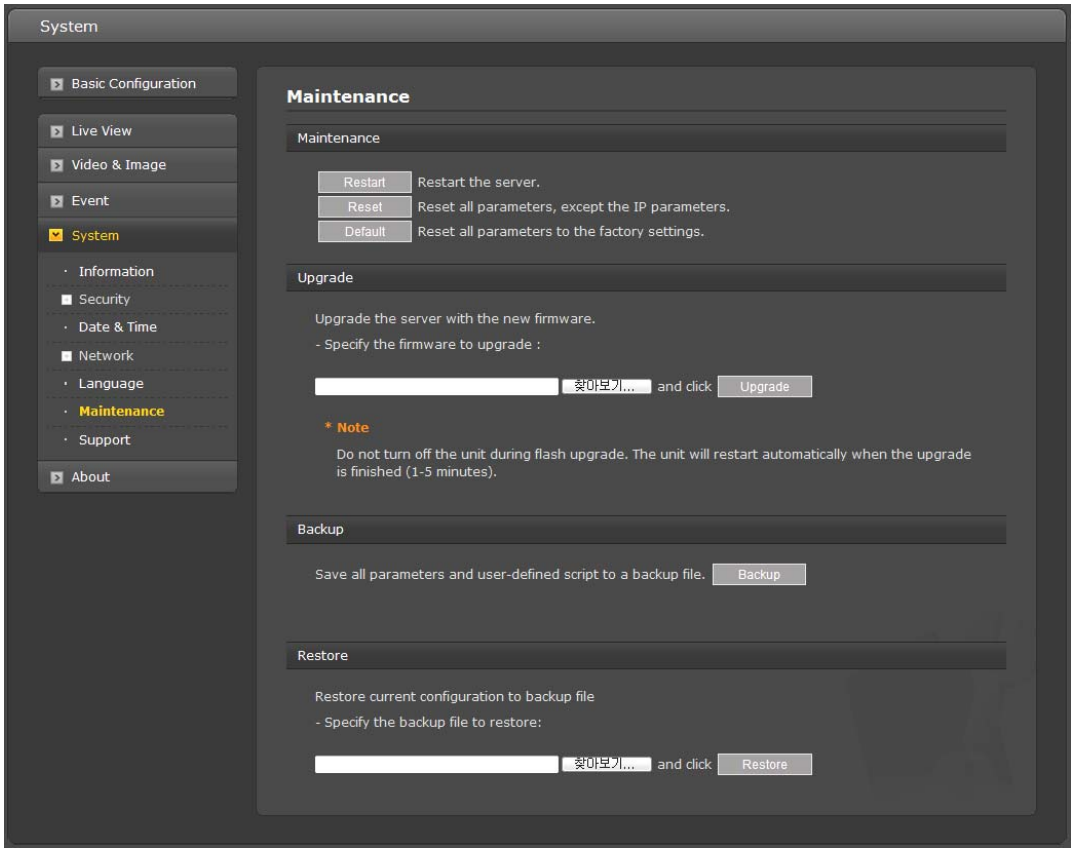
5) Language

Select a user language. This has English, Russian, Korean and Chinese.



When the settings are complete, click **Save**, or click **Reset** to revert to previously saved settings.

6) Maintenance



- **Maintenance**
  - **Restart:** The unit is restarted without changing any of the settings. Use this method if the unit is not behaving as expected.
  - **Reset:** The unit is restarted and most current settings are reset to factory default values. The settings that are not affected are:
    * the boot protocol (DHCP or static)
    * the static IP address
    * the default router
    * the subnet mask
    * the system time
  - **Default:** The default button should be used with caution. Pressing this will return all of the network camera's settings to the factory default values (including the IP address).

- **Upgrade**
  Upgrade the camera by importing an upgrade file and pressing the **Upgrade** button. During the upgrade, do not turn off the power to the network camera. After waiting five minutes or longer, try to access the camera again.

  To perform an update for multiple cameras at one time, use the SmartManager discovery and update tool and select them using the SHIFT and CTRL keys (see SmartManager manual for details).

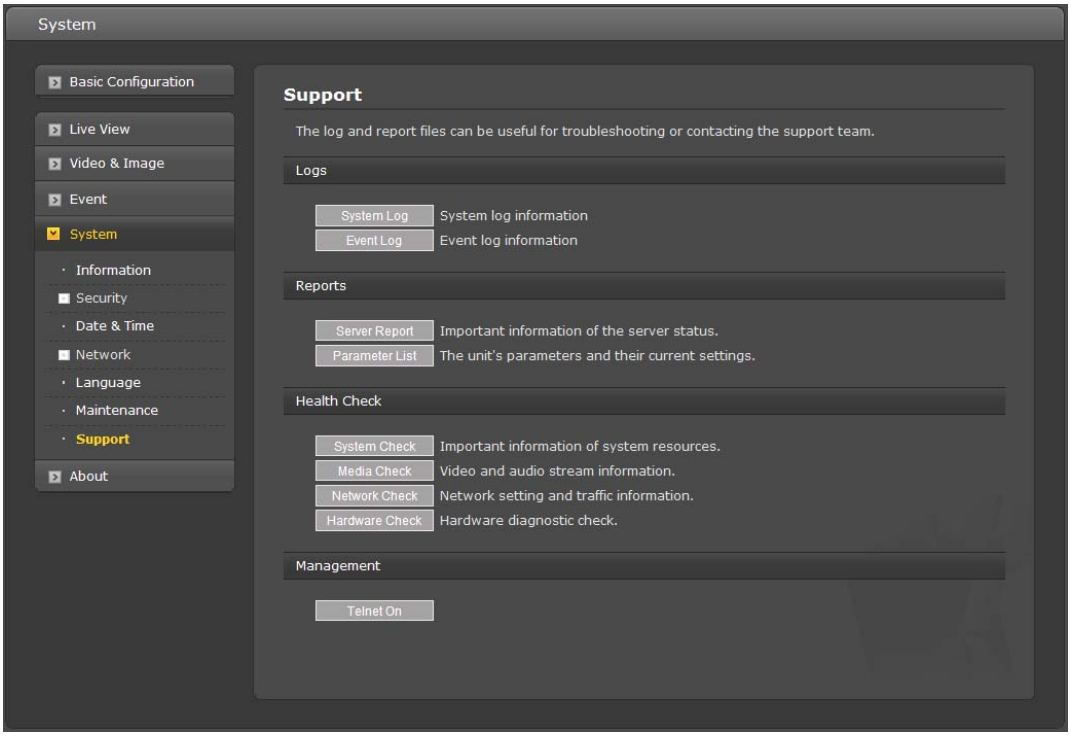
- **Backup**
  Click the **Backup** button to save setting values that users enter to the network camera to a user PC.

- **Restore**
  Click the **Restore** button to import and apply setting values saved to a user PC.

  Note: Backup and Restore can only be used on the same unit running the same firmware. This feature is not intended for multi-configurations or for firmware upgrades.

7) Support

The support page provides valuable information on troubleshooting and contact information, should you require technical assistance.

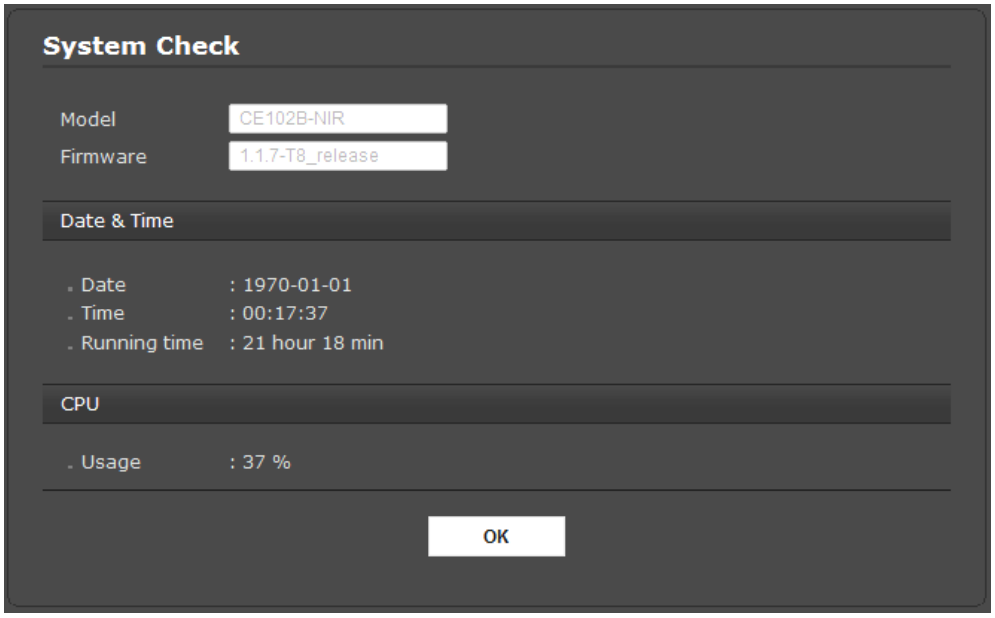


- **Logs**
  The network camera supports system log information. Click the System Log button to get the log data.

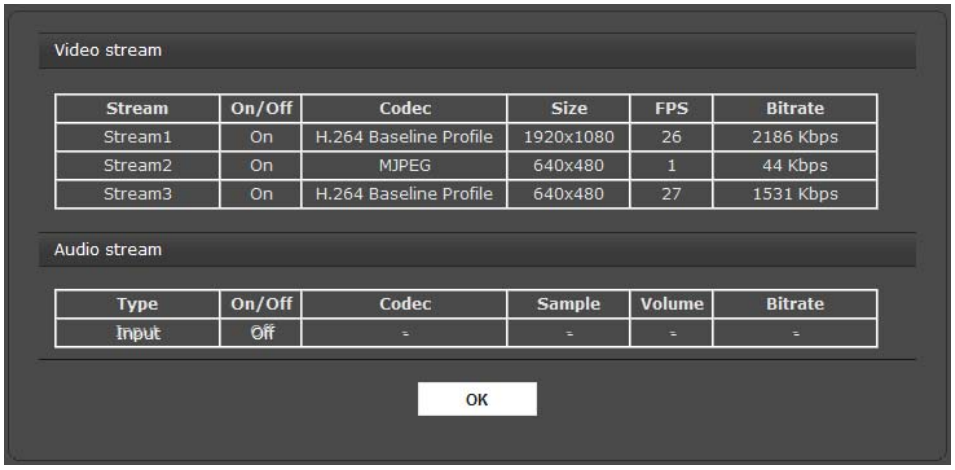
- **Reports**
  - **Server Report:** Click the Server Report button to get the important information about the server's status and should always be included when requesting support.
  - **Parameter List:** Click the Parameter List button to see the unit's parameters and their current settings.

- **Health Check**

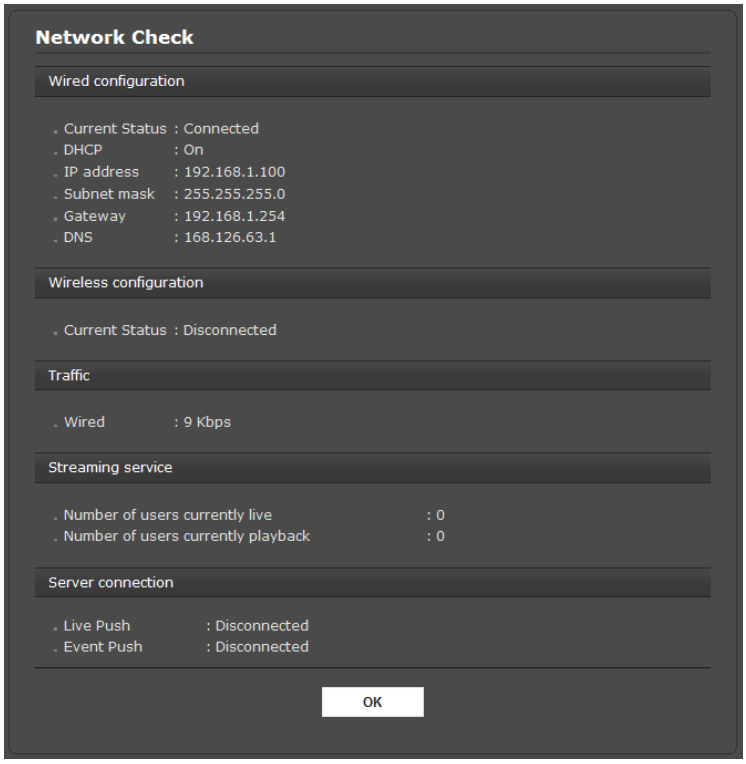
  - **System Check:** Click the System Check button to get the important information about the camera's system resources. The pop-up window displays as below.



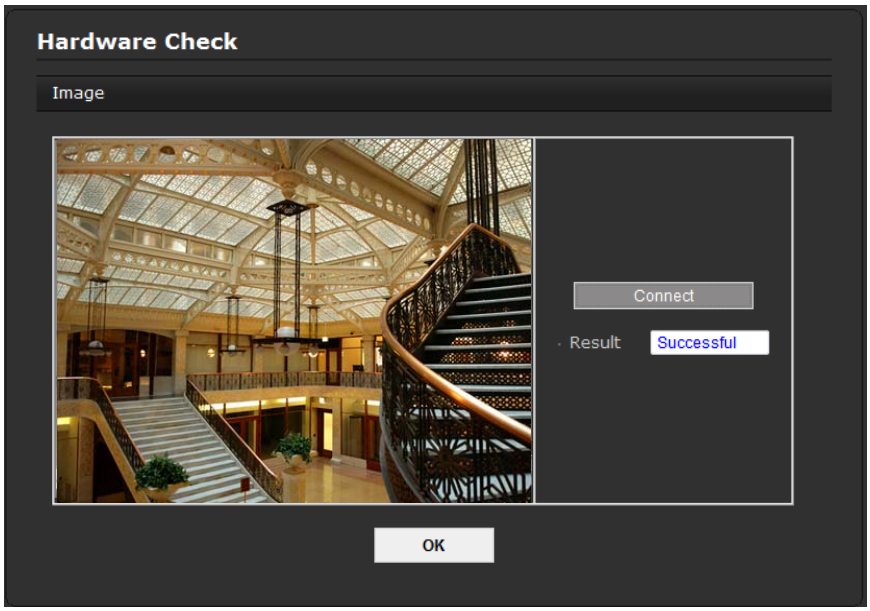
- **Media Check:** Click the Media Check button to get the information about the camera's video stream. The pop-up window displays as below.


Video stream
Stream | On/Off | Codec | Size | FPS | Bitrate
Stream1 | On | H.264 Baseline Profile | 1920x1080 | 26 | 2186 Kbps
Stream2 | On | MJPEG | 640x480 | 1 | 44 Kbps
Stream3 | On | H.264 Baseline Profile | 640x480 | 27 | 1531 Kbps
Audio stream
Type | On/Off | Codec | Sample | Volume | Bitrate
Input | Off | - | - | - | -
OK

- **Networks Check:** Click the Network Check button to get the information about the camera's network setting and traffic. The pop-up window displays as below.

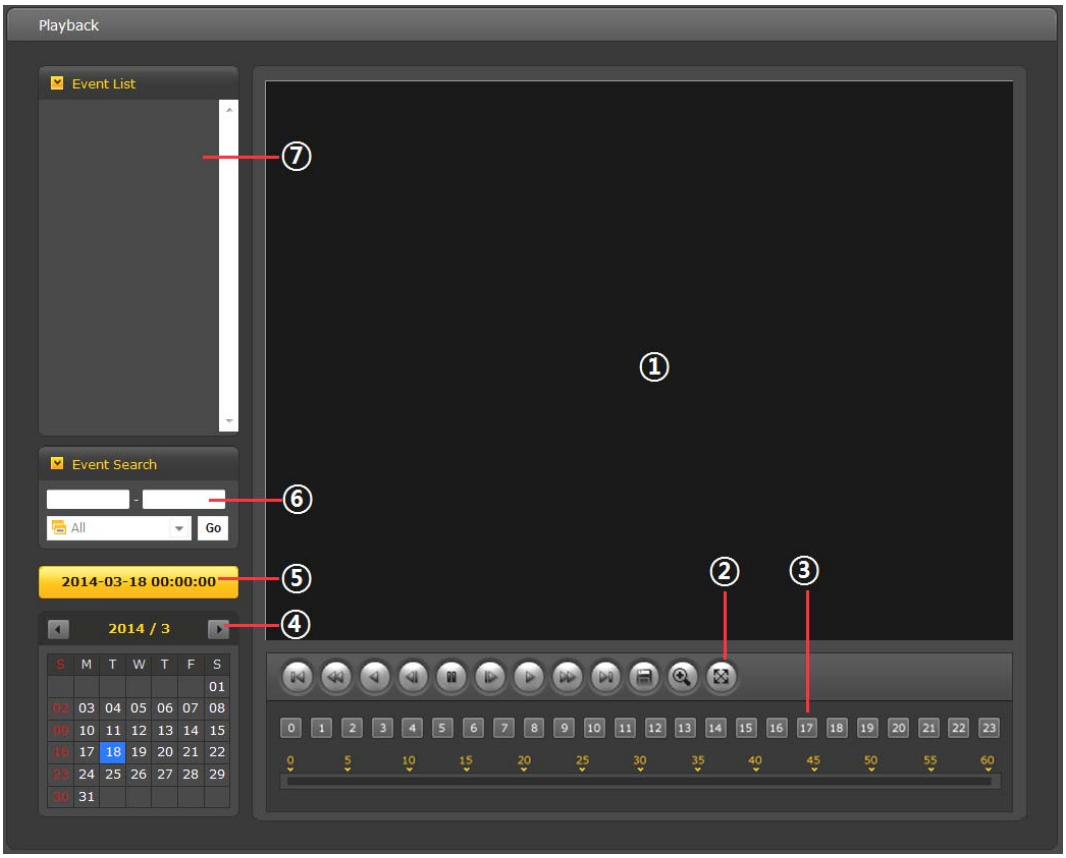


- **Hardware Check:** Click the Hardware Check button to diagnose the camera's hardware, such as video.



3.6 Playback

The Playback window contains a list of recordings made to the memory card. It shows each recording's start time, length, the event type used to start the recording, calendar and time slice bar indicates if the recording exists or not.



The description of playback window follows.

(1) Video Screen

You can see the video screen when playing the video clip from the Micro SD memory

(2) Playback Buttons

To view a recording from the SD local storage, select it from the list and click the Playback buttons.

- Go to First: go to the beginning of the video clip.
- Fast Backward: fast play backward (rewind) of the video clip.
- Backward: play the video clip backward.
- Backward Step: go back one frame of the video clip.
- Pause: temporarily stop (pause) playback of the video clip.
- Forward Step: go forward one frame of the video clip.
- Forward: play the video clip forward.
- Fast Forward: fast forward: play the video clip in fast forward.
- Go to Last: go to the end of the video clip.

Clip copy: copy the video clip.

Zoom In: zoom in the video clip

Full Screen: display full screen of the video.

(3) Time Chart

Display an hour-based search screen for the chosen date. If there is recording data, a blue section will be displayed on a 24-hour basis. If you select a particular hour in the chart, a yellow square on the hour will be displayed.

(4) Search Calendar

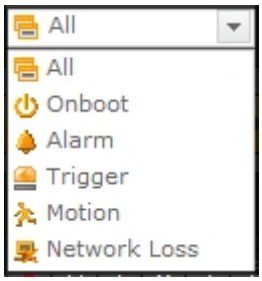
Search results from the SD local storage in the network camera connected are displayed monthly. If there is a recorded data for a particular date, a blue square on the date will be displayed.

(5) Play Time

Displays time of the video playing.

(6) Event Search Window

Select a search option in the drop-down list and click **Go** button. You can also enter the time period for searching. If you click Start Date or End Date zone, displays Search Calendar.

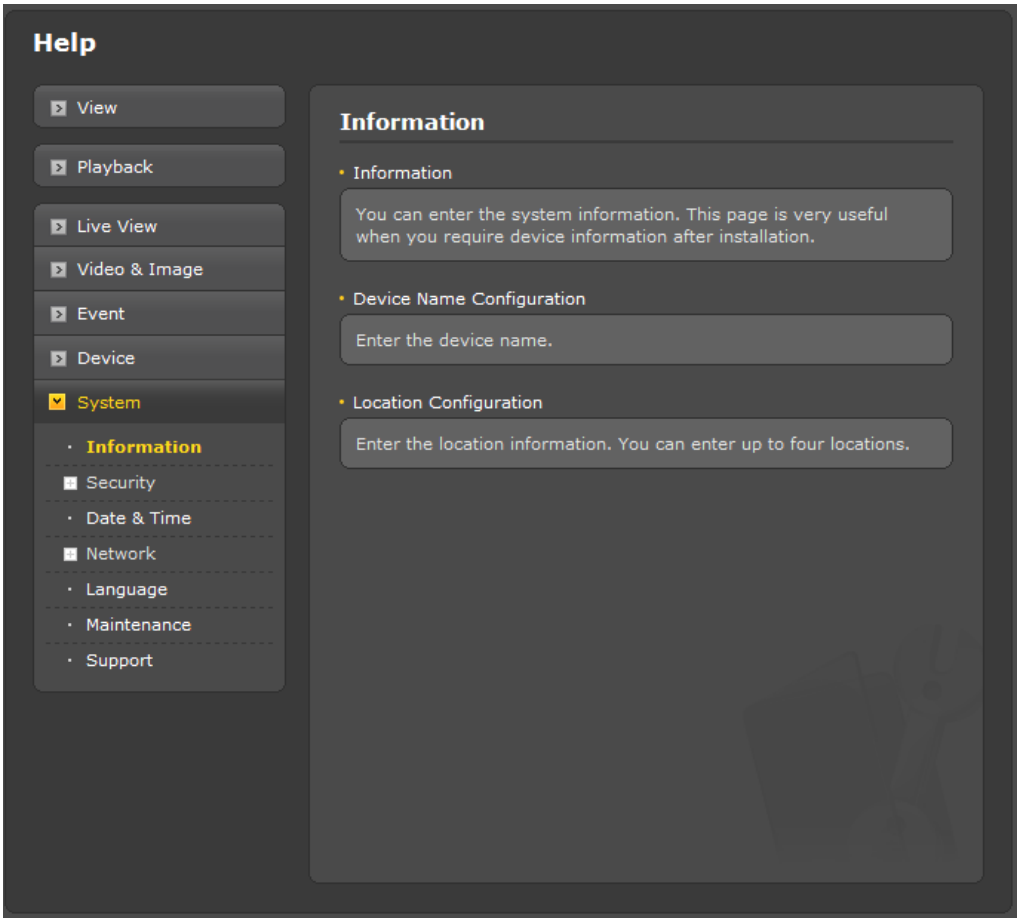


(7) Event List Window

Event List displays the event(s) that were recorded in the SD local storage. Select a list and click the play button. The video clip will be played.

3.7 Help

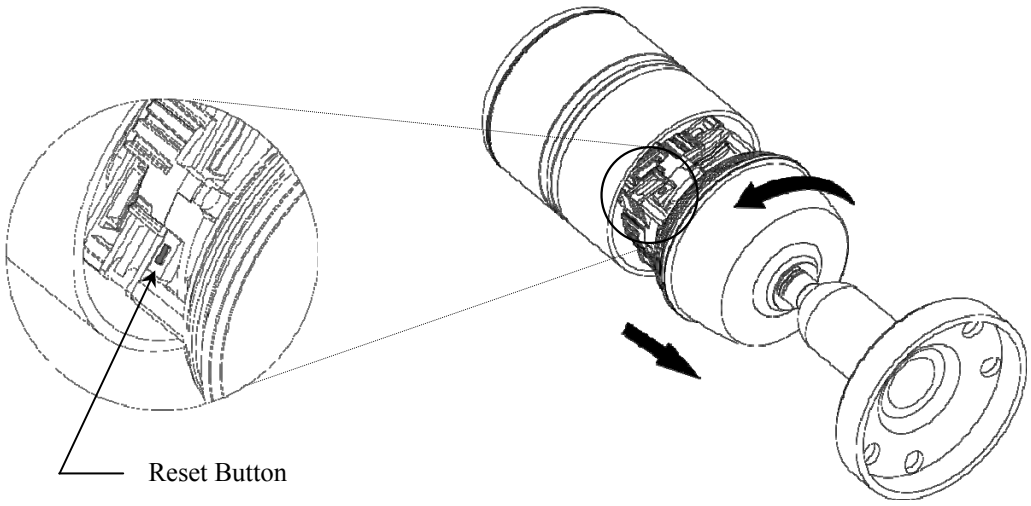
The Help information window will be provided as a popup window so that users can open and read it without a need for log-in. It will offer a description on setting and Help page by which users can manipulate the network camera without a reference to the manual.



3.8 Resetting to the factory default settings

To reset the network camera to the original factory settings, go to the Setup>System >Maintenance web page (described in “3.5.6 System>Maintenance” of the User’s Manual) or use the Reset button on the network camera, as described below:

Follow the instructions below to reset the network camera to the factory default settings using the Reset button.



Remove the front cap

- **Using the Reset Button**
  Follow the instructions below to reset the network camera to the factory default settings using the Reset button.

  1. Switch off the network camera by disconnecting the power adapter.
  2. Remove the front cap of the camera.
  3. Press and hold the Reset button while reconnecting the power.
  4. Keep the Reset button pressed for at least 2 seconds.
  5. Release the Reset button.
  6. The network camera resets to factory defaults and restarts after completing the factory reset.
  7. Close the front cap of the camera.

Caution: When performing a Factory Reset, you will lose any settings you have saved.

4. Appendix

4.1 Troubleshooting

Troubleshooting if problems occur, verify the installation of the network camera with the instructions in this manual and with other operating equipment. Isolate the problem to the specific piece of equipment in the system and refer to the equipment manual for further information.

Problems/Symptoms	Possible Causes or Corrective Actions
The camera cannot be accessed by some clients.	If using a proxy server, try disabling the proxy setting in your browser. Check all cabling and connectors.
The camera works locally, but not externally.	Check if there are firewall settings that need to be adjusted. Check if there are router settings that need to be configured.
Poor or intermittent network connection.	If using a network switch, check that the port on that device uses the same setting for the network connection type (speed/duplex).
The camera cannot be accessed via a host name.	Check that the host name and DNS server settings are correct.
Not possible to log in.	When HTTPS is enabled, ensure that the correct protocol (HTTP or HTTPS) is used. When attempting to log in, you may need to manually type in http or https in the browser's address bar.
No image using Refresh and/or slow updating of images.	If images are very complex, try limiting the number of clients accessing the camera.
Images only shown in black & white.	Check the Video & Image setting.
Blurred images.	Refocus the camera.
Poor image quality.	Increased lighting can often improve image quality. Check that there is sufficient lighting at the monitored location. Check all image and lighting settings.
Rolling dark bands or flickering in image.	Try adjusting the Exposure Control setting under AE and AWB part.
H.264 not displayed in the client.	Check that the correct network interface is selected in the Video & Image/Stream.
Multicast H.264 not displayed in the client.	Check with your network administrator that the multicast addresses used by the camera are valid for your network. Check that the Enable multicast checkbox are enabled in the System/Network/RTP tab. Checks with your network administrator to see if there is a firewall preventing viewing.
Multicast H.264 only accessible by local clients.	Check if your router supports multicasting, or if the router settings between the client and the server need to be configured. The TTL value may need to be increased.
Color saturation is different in H.264 and Motion JPEG.	Modify the settings for your graphics adapter. Please see the adapter's documentation for more information.
Video cannot be recorded.	Check that the SD Card is inserted properly. Check that the SD Card is formatted properly.

4.2 Preventive Maintenance

Preventive maintenance allows detection and correction of minor that faults before they become serious and cause equipment failure.

Every three months, perform the following maintenance.

1. Inspect all connection cables for deterioration or other damage.
2. Clean components with a clean damp cloth.
3. Verify that all the mounting hardware is secure.

4.3 Product Specification

Main Item		Specification
CAMERA	Image sensor	1/2.8” Progressive scan RGB CMOS
	Active Array	1920(H) x 1080(V)
	Lens	Fixed 3.7mm Lens, F1.8
	Angle of View	90.0°(H) x 50.0(V)
	IR Distance	65 ft (20 m) (with built-in 24 IR LEDs)
	Min. illumination	Color: 0.2Lux, B/W: 0.0Lux (F1.8, 50IRE with IR On)
	Shutter Speed	1/20,000 ~ 1/30 (Slow shutter 1/15, 1/8 and 1/4)
NETWORK	Video Compression	-. Motion JPEG -. MPEG-4 Part2 -. H.264 (MPEG-4 Part 10) -. Profiles: H.264 HP, MP, and BP, MPEG-4 SP
	Video Streaming	Simultaneously H.264(or MPEG-4) and M-JPEG Controllable Frame Rate and Bandwidth VBR/CBR H.264 and MPEG-4
	Video Resolutions	1920x1080 ~ 320x240
	Frame Rate	30fps @ all resolution
	Protocol	TCP/IP, UDP, IPv4/v6, HTTP, HTTPS, QoS, FTP, uPnP, RTP, RTSP, RTCP, DHCP, ARP, Zeroconf, Bonjour
	Security	Multi-user authority, HTTPS, IP Filtering, Privacy Zone
	Max. Connection	10
	API Programming Interface	API Supported, Open Platform Compatible: ONVIF
	Alarm Events	-. File upload via FTP and HTTP -. Notification via E-mail, HTTP and TCP
	Video Buffering	Pre and Post Alarm
	Motion Detection	Yes, max. 8 programmable zone
	Network Time Synchronization	Yes
	SD Recording	Yes, Continuous/Event
	Software Reset	Yes
	Factory Reset	Yes, Button/Web browser
	Auto Recovery	Yes
	Installation Tool	SmartManager
	Upgrade	Web browser, SmartManager
GENERAL	Ethernet	RJ-45 10BASE-T/100BASE-TX
	Operating Temperature	14°F ~ 113°F (-10°C ~ 45°C)
	Operation Humidity	0~80% (non-condensing)
	Power Consumption	12 VDC: 500mA, 6.0W; PoE: 125mA, 6.0W (with IR on) Power over Ethernet IEEE 802.3af Class0
	Dimensions (WxHXD)	2.9x3.3x6.8 in. (74.21x84x173 mm); Diam: 2.6 in. (66 mm)
	Unit Weight	1 lb (454g)

System Requirement for Web Browser

Operating System: Microsoft Windows OS Series
CPU: Intel Core 2 Duo 2Ghz or higher, 1GB RAM or more, 10GB free disk or higher
VGA: AGP, Video RAM 32MB or higher (1024x768, 24bpp or higher)

General performance considerations

When setting up your system, it is important to consider how various settings and situations will affect performance. Some factors affect the amount of bandwidth (the bit rate) required, others can affect the frame rate, and some affect both. If the load on the CPU reaches its maximum, this will also affect the frame rate.

The following factors are among the most important to consider:

-. High image resolutions and/or lower compression levels (or high bitrates) result in larger images. Frame rate and Bandwidth affected.
-. Accessing both Motion JPEG and H.264 video streams simultaneously. Frame rate and bandwidth affected.
-. Heavy network utilization due to poor infrastructure. Frame rate and Bandwidth affected.
-. Heavy network utilization via wireless router due to poor infrastructure. Frame rate and bandwidth affected.
-. Viewing on poorly performing client PCs lowers perceived performance. Frame rate affected.

Shipping Instructions

Use the following procedure when returning a unit to the factory:

1. Call or write Vicon for a Return Authorization (R.A.) at one of the locations listed below. Record the name of the Vicon employee who issued the R.A.

   Vicon Industries Inc.
   131 Heartland Boulevard
   Edgewood, NY 11717
   Phone: 631-952-2288; Toll-Free: 1-800-645-9116; Fax: 631-951-2288

   For service or returns from countries in Europe, contact:

   Vicon Industries (U.K.) Ltd
   Brunel Way
   Fareham, PO15 5TX
   United Kingdom
   Phone: +44 (0)1489/566300; Fax: +44 (0)1489/566322

2. Attach a sheet of paper to the unit with the following information:

   a. Name and address of the company returning the unit
   b. Name of the Vicon employee who issued the R.A.
   c. R. A. number
   d. Brief description of the installation
   e. Complete description of the problem and circumstances under which it occurs
   f. Unit's original date of purchase, if still under warranty

3. Pack the unit carefully. Use the original shipping carton or its equivalent for maximum protection.
4. Mark the R.A. number on the outside of the carton on the shipping label.

Vicon Standard Equipment Warranty

Vicon Industries Inc. (the "Company") warrants your equipment to be free from defects in material and workmanship under Normal Use from the date of original retail purchase for a period of three years, with the following exceptions:

1. Monitors, all models: One year from date of original retail purchase.
2. Uninterruptible Power Supplies: Two years from date of original retail purchase.
3. VDR-700 Recorder Series: One year from date of original retail purchase.
4. V5616MUX: One year from date of original retail purchase.
5. Arecont Cameras: One year from date of original retail purchase.
6. FMC series fiber-optic media converters and associated accessories: Lifetime warranty.
7. For PTZ cameras, "Normal Use" excludes prolonged use of lens and pan-and-tilt motors, gear heads, and gears due to continuous use of "autopan" or "tour" modes of operation. Such continuous operation is outside the scope of this warranty.
8. Any product sold as "special" or not listed in Vicon's commercial price list: One year from date of original retail purchase.

Date of retail purchase is the date original end-user takes possession of the equipment, or, at the sole discretion of the Company, the date the equipment first becomes operational by the original end-user.

The sole remedy under this Warranty is that defective equipment be repaired or (at the Company's option) replaced, at Company repair centers, provided the equipment has been authorized for return by the Company, and the return shipment is prepaid in accordance with policy.

The Company will not be obligated to repair or replace equipment showing abuse or damage, or to parts which in the judgment of the Company are not defective, or any equipment which may have been tampered with, altered, misused, or been subject to unauthorized repair.

Software supplied either separately or in hardware is furnished on an "As Is" basis. Vicon does not warrant that such software shall be error (bug) free. Software support via telephone, if provided at no cost, may be discontinued at any time without notice at Vicon's sole discretion. Vicon reserves the right to make changes to its software in any of its products at any time and without notice.

This Warranty is in lieu of all other conditions and warranties express or implied as to the Goods, including any warranty of merchantability or fitness and the remedy specified in this Warranty is in lieu of all other remedies available to the Purchaser.

No one is authorized to assume any liability on behalf of the Company, or impose any obligations on it in connection with the sale of any Goods, other than that which is specified above. In no event will the Company be liable for indirect, special, incidental, consequential, or other damages, whether arising from interrupted equipment operation, loss of data, replacement of equipment or software, costs or repairs undertaken by the Purchaser, or other causes.

This warranty applies to all sales made by the Company or its dealers and shall be governed by the laws of New York State without regard to its conflict of laws principles. This Warranty shall be enforceable against the Company only in the courts located in the State of New York.

The form of this Warranty is effective May 4, 2012.

THE TERMS OF THIS WARRANTY APPLY ONLY TO SALES MADE WHILE THIS WARRANTY IS IN EFFECT. THIS WARRANTY SHALL BE OF NO EFFECT IF AT THE TIME OF SALE A DIFFERENT WARRANTY IS POSTED ON THE COMPANY'S WEBSITE, *WWW.VICON-SECURITY.COM*. IN THAT EVENT, THE TERMS OF THE POSTED WARRANTY SHALL APPLY EXCLUSIVELY.

Vicon Part Number: 8006-9010-03-10 Rev 0512

Vicon Industries Inc.

Internet Address: www.vicon-security.com

VICON

CE102B Network Outdoor Bullet Camera